53-1003755-01
November 2014

Brocade Flexible Authentication

Deployment Guide

Notice: This document is for informational purposes only and does not set forth any warranty, expressed or implied, concerning any equipment, equipment feature, or service offered or to be offered by Brocade. Brocade reserves the right to make changes to this document at any time, without notice, and assumes no responsibility for its use. This informational document describes features that may not be currently available. Contact a Brocade sales office for information on feature and product availability. Export of technical data contained in this document may require an export license from the United States government.

The authors and Brocade Communications Systems, Inc. assume no liability or responsibility to any person or entity with respect to the accuracy of this document or any loss, cost, liability, or damages arising from the information contained herein or the computer programs that accompany it.

The product described by this document may contain open source software covered by the GNU General Public License or other open source license agreements. To find out which open source software is included in Brocade products, view the licensing terms applicable to the open source software, and obtain a copy of the programming source code, please visit http://www.brocade.com/support/oscd.

Contents

Brocade Flexible Authentication Deployment Guide

Preface

In software releases prior to FI 8.0.20, when 802.1X and MAC authentication are both configured on the same port, both MAC authentication and 802.1X method are attempted for the clients. This may result in additional authentication traffic on the network. To solve this issue, Brocade introduced Flexible authentication feature.

Flexible authentication allows the network administrator to set the sequence of the authentication methods to be attempted on a switch port. This feature supports two methods - 802.1X and MAC authentication. By default the sequence is set to 802.1X followed by MAC authentication. 802.1X is attempted first. If the client is not 802.1X capable, MAC authentication is attempted. When the sequence is set to MAC authentication followed by 802.1X, both methods are attempted for the clients. This option should help customers to upgrade their Brocade devices from previous releases to FI 8.0.20, and retain the same functionality.

Brocade's flexible authentication implementation allows each client connected to the same switch port, to have different network policy (such as dynamic VLAN or ingress IPv4 ACL). This is achieved by using MAC-based VLANs that allow the creation of VLANs based on MAC addresses instead of traditional method of port membership.

Overview

802.1X Port Security

Brocade FastIron switches support IEEE 802.1X standard for authenticating devices attached to LAN ports. The 802.1X standard defines three types of device roles in a network:

- Client/Supplicant
- Authenticator
- Authentication Server

Client/Supplicant: The devices (for example, Desktop/laptop, IP phone etc.) that seek to gain access to the network. Clients must be running software that supports the 802.1X standard. Clients can either be directly connected to a port on the Authenticator, or can be connected by way of a hub.

Authenticator: The device that controls access to the network. In an 802.1X configuration, the Brocade device serves as the Authenticator. The Authenticator passes messages between the Client and the Authentication Server. Based on the identity information supplied by the Client, and the authentication information supplied by the Authentication Server, the Authenticator either grants or restricts network access to the Client.

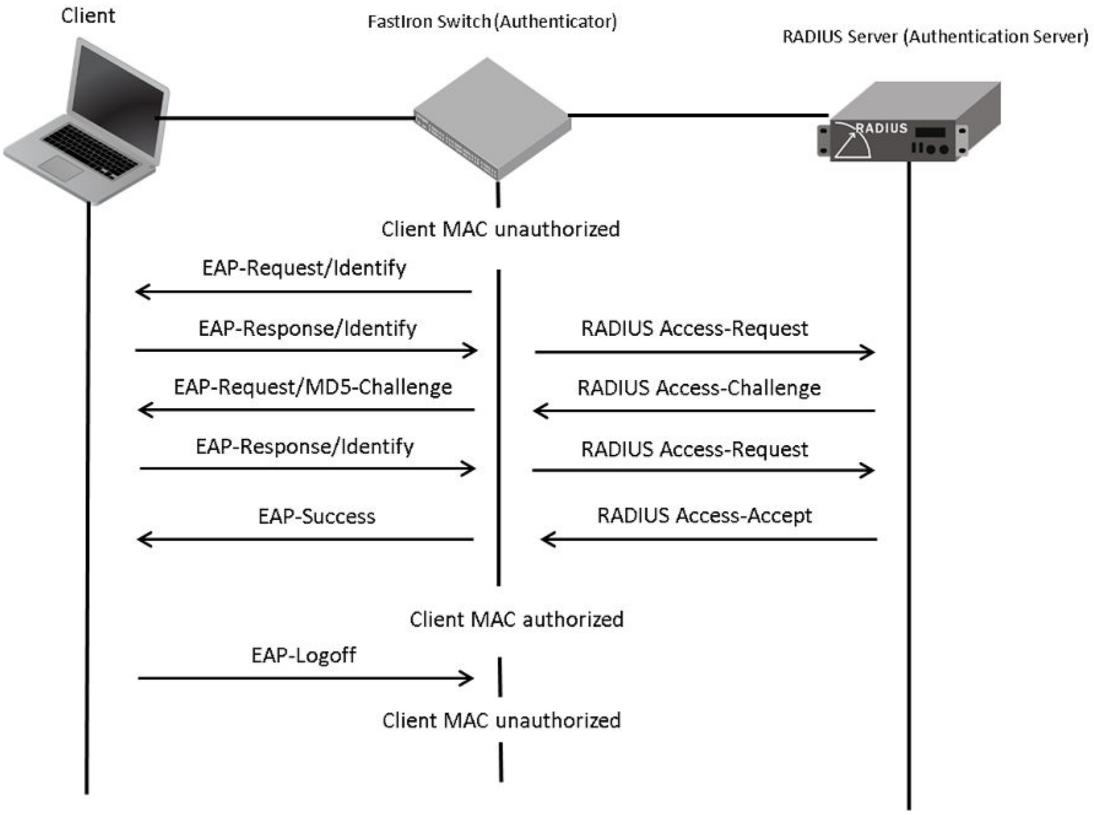
Authentication Server: The device that validates the Client and specifies whether or not the Client may access services on the device. Brocade supports Authentication Servers running RADIUS

Message exchange during authentication

For communication between the devices, 802.1X port security uses the Extensible Authentication Protocol (EAP), defined in RFC 2284. The 802.1X standard specifies a method for encapsulating EAP messages so that they can be carried over a LAN. This encapsulated form of EAP is known as EAP over LAN (EAPOL). During authentication, EAPOL messages are exchanged between the Supplicant and the Authenticator, and RADIUS messages are exchanged between the Authenticator and the Authentication Server.

The following figure illustrates a sample exchange of messages between an 802.1X-enabled Client, a FastIron switch acting as Authenticator, and a RADIUS server acting as an Authentication Server.

FIGURE 1 Message exchange between client, authenticator, and authentication server



In this example, the Authenticator (the FastIron switch) initiates communication with an 802.1X-enabled Client. When the Client responds, it is prompted for a username (255 characters maximum) and password. The Authenticator passes this information to the Authentication Server, which determines whether the Client can access services provided by the Authenticator. If authentication is successful, MAC address of the client is authorized. In addition, RADIUS server may include network access policy such as dynamic VLAN or ingress IPv4 ACL in the access-accept message for this client. When the Client logs off, the MAC address of the client becomes unauthorized again.

A client may fail to get authenticated in various scenarios. The scenarios and options available to place the client in various VLANs due to authentication failure are described below.

Guest VLAN: The client is moved to a Guest VLAN when it does not respond to the 802.1X requests for authentication. It is possible that the client does not have the 802.1X authenticator loaded and hence needs some way to access the network, from where it can download the authenticator. The administrator can configure the Guest VLAN with such access and other access methods, as required.

Critical VLAN: There may be scenarios in which the RADIUS server is not available and authentication fails. This can happen the first time the client is authenticating or when it re-authenticates. The administrator can decide to grant some or the same access as original in this situation instead of blocking the access. This VLAN should be configured with the desired access levels.

Restricted VLAN: When the authentication fails, the client can be moved into a restricted VLAN instead of failing completely. The administrator may decide to grant some access in this scenario, instead of blocking the access. This VLAN should be configured with the desired access levels.

For more information about 802.1X feature, please refer to FastIron 8.0.20 security guide.

MAC Authentication

The MAC authentication feature is a mechanism by which incoming traffic originating from a specific MAC address is forwarded by the Brocade switch only if the source MAC address is successfully authenticated by a RADIUS server. The MAC address itself is used as the username and password for RADIUS authentication; the user does not need to provide a specific username and password to gain access to the network. If RADIUS authentication for the MAC address is successful, traffic from the MAC address is forwarded in hardware.

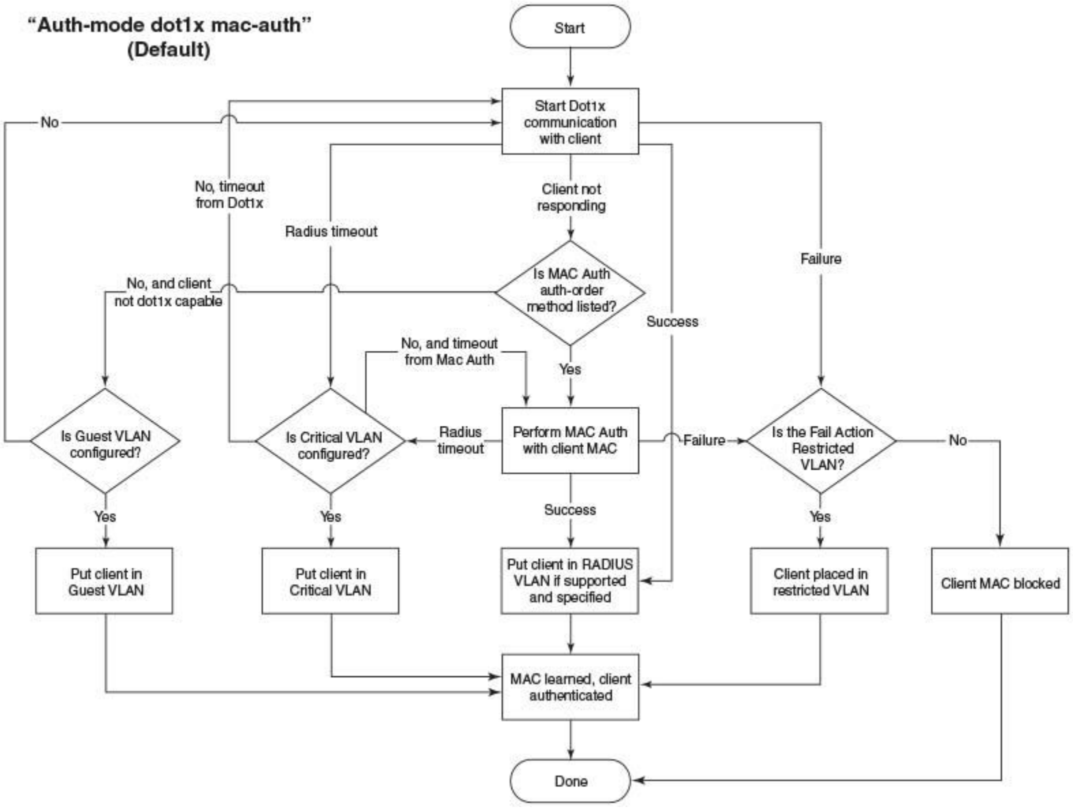
If the RADIUS server cannot validate the user's MAC address, then it is considered an authentication failure, and a specified authentication-failure action can be taken. The format of the MAC address sent to the RADIUS server is configurable through the CLI. MAC authentication feature supports the use of critical VLAN and restricted VLAN as described in section 2.1.

For more information about MAC authentication feature, please refer to the FastIron 8.0.20 security guide.

How Flexible Authentication works

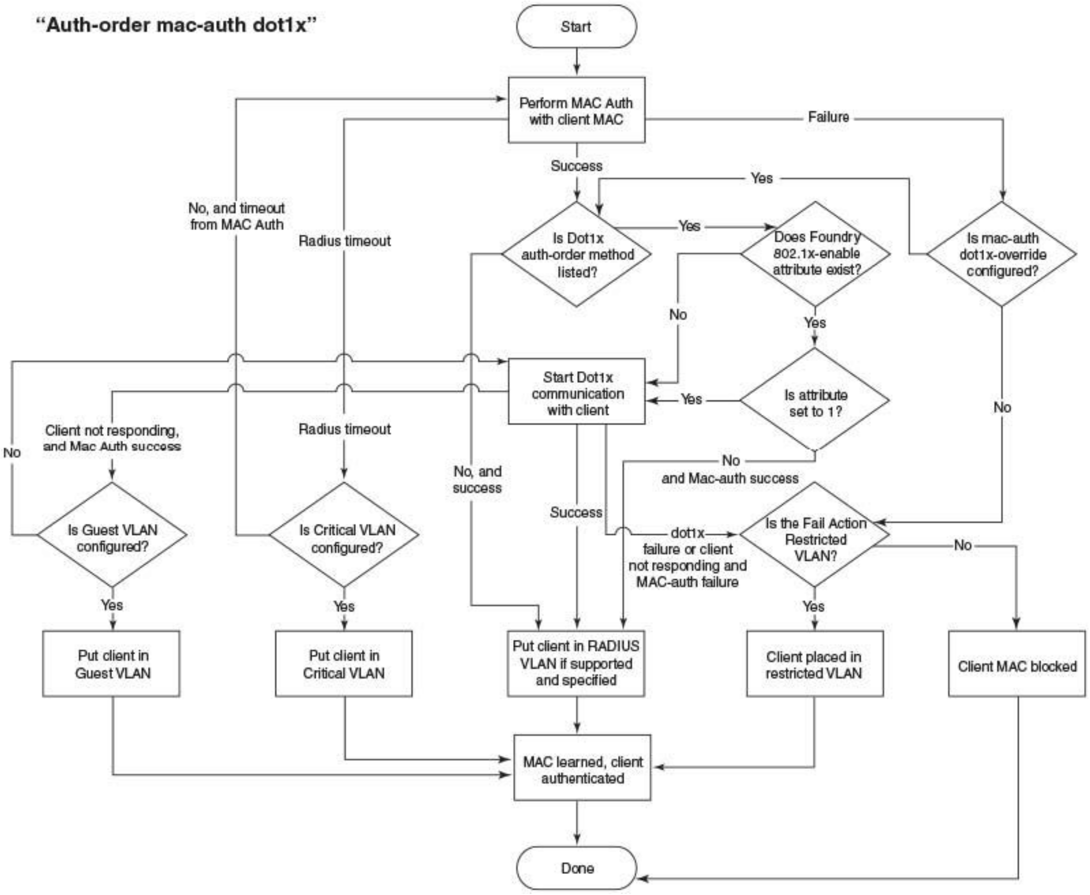
- By default the sequence is set to 802.1X followed by MAC authentication. 802.1X is attempted first. If the client is not 802.1X capable, MAC authentication is attempted.

FIGURE 2 Default sequence - 802.1X followed by MAC authentication


"Auth-mode dot1x mac-auth"
(Default)
Start
Start Dot1x communication with client
No
No, timeout from Dot1x
Radius timeout
Client not responding
Failure
Is MAC Auth auth-order method listed?
No, and client not dot1x capable
Success
No, and timeout from Mac Auth
Yes
Is Guest VLAN configured?
Is Critical VLAN configured?
Radius timeout
Perform MAC Auth with client MAC
Failure
Is the Fail Action Restricted VLAN?
No
Yes
Yes
Success
Yes
Put client in Guest VLAN
Put client in Critical VLAN
Put client in RADIUS VLAN if supported and specified
Client placed in restricted VLAN
Client MAC blocked
MAC learned, client authenticated
Done

- When the sequence is set to MAC authentication followed 802.1X
  - MAC authentication is attempted first. If it succeeds, 802.1X method is also attempted.
  - If MAC authentication method succeeds, 802.1X process can be skipped by using a vendor specific RADIUS attribute called "Foundry-802_1x-enable" for the MAC authentication process. If this attribute is present in RADIUS access-accept message during MAC authentication and the value of this attribute is set to 1, 802.1X is not attempted for the client
  - If MAC authentication method fails, 802.1X is not attempted and configured failure action is taken. However, administrator can configure dot1x-override through the CLI to allow the clients that failed MAC authentication, authenticate via 802.1X method

FIGURE 3 MAC authentication followed by 802.1X


"Auth-order mac-auth dot1x"
Start
Perform MAC Auth with client MAC
Failure
Success
Yes
No, and timeout from MAC Auth
Radius timeout
Is Dot1x auth-order method listed?
Yes
Does Foundry 802.1x-enable attribute exist?
Is mac-auth dot1x-override configured?
No
Yes
Start Dot1x communication with client
Yes
Is attribute set to 1?
No
Client not responding, and Mac Auth success
Radius timeout
No
No, and success
No
and Mac-auth success
Success
Is Guest VLAN configured?
Is Critical VLAN configured?
dot1x failure or client not responding and MAC-auth failure
Is the Fail Action Restricted VLAN?
No
Yes
Yes
Yes
Put client in Guest VLAN
Put client in Critical VLAN
Put client in RADIUS VLAN if supported and specified
Client placed in restricted VLAN
Client MAC blocked
MAC learned, client authenticated
Done

Supported Platforms

Flexible authentication support was introduced in release FI 08.0.20. Supported platforms are FCX, ICX6610, ICX6430, ICX6450, ICX7750, and ICX7450. By default, FCX, ICX6610, ICX6430, ICX6450 platforms support two clients per port. It can be changed to support 32 clients per port through the CLI. ICX6450 and ICX7750 support 32 clients per port by default.

Purpose of the document

The purpose of this deployment guide is to provide an understanding of FlexAuth along with the steps required to successfully deploy a strong authentication scheme. This guide describes three use cases:

1. Dynamic VLAN and ACL assignment with default authentication order, 802.1X followed by MAC authentication

   This is Brocade recommended configuration. This use case describes how to enabled flexible authentication on a switch that uses 802.1X as first method to authenticate the clients and MAC authentication as a failover authentication method.
2. Dynamic VLAN and ACL assignment with authentication order – MAC authentication followed by 802.1X

In releases prior to FI 8.0.20, when 802.1X and MAC authentication were both configured on the same port, both MAC authentication and 802.1X method were attempted for the clients. This use case should help the customers to upgrade their Brocade devices from previous releases to FI 8.0.20, and retain the same functionality.

3. Authenticating a 802.1X phone and a PC on the same port

The radius configuration to deploy this scenario differs for each vendor. This use case shows how to deploy a typical VoIP network with 802.1X using Brocade devices.

Audience

The document can be used by technical marketing engineers, system engineers, technical assistance center engineers and customers deploy a flexible authentication scheme for a network.

Related documents

- FastIron 8020 Security Guide
- IEE 802.1X-2004

  http://www.ieee802.org/1/pages/802.1x-2004.html
- Extensible Authentication Protocol (EAP)

  http://tools.ietf.org/html/rfc2284
- Remote Authentication Dial in User Service (RADIUS)

  http://tools.ietf.org/html/rfc2865
- RADIUS Extensions

  http://tools.ietf.org/html/rfc2869

Document history

Date	Version	Description
10/8/2014	1.0	Initial release
10/16/2014	1.1	Added the section "Deployment consideration"
10/27/2014	1.2	Added the section "Upgrade consideration"
11/6/2014	1.3	Added screen shots of RADIUS configuration to Use Case 1 and Use Case 2

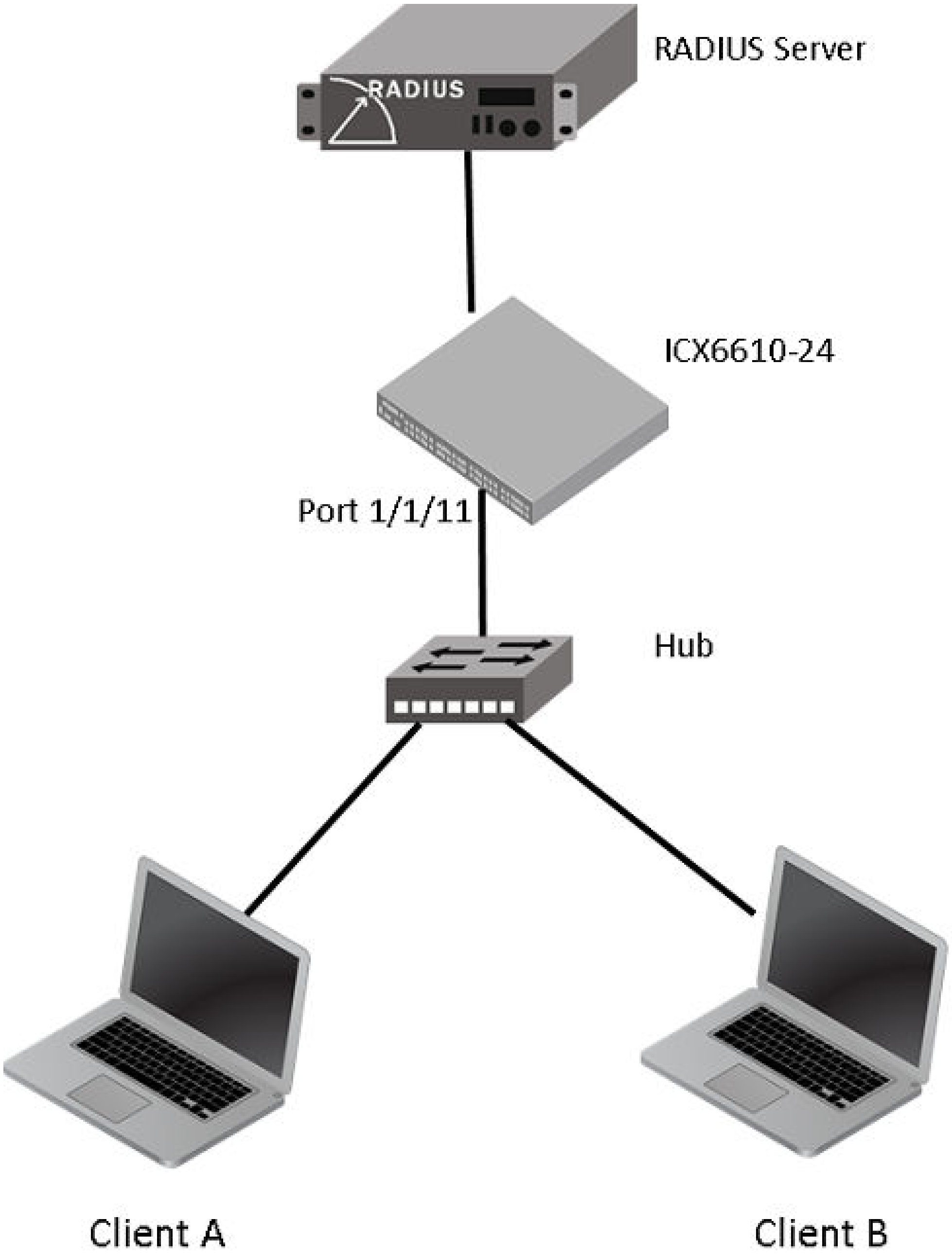
Use Case 1: Dynamic VLAN and ACL assignment with default authentication order

This use case demonstrates the capability of a Brocade switch to maintain different network policies for each client connected to the same port. The flexible authentication order is set to default (802.1X followed by MAC authentication). In topology A, there are two clients (Client A and Client B) connected to port 1/1/11 of an ICX6610-24 via hub. The hub is used to connect two clients to the same port.

ICX6610-24 has IP connectivity to the RADIUS server. The server's IP address is 10.20.64.208. In this topology, network policy server on a PC running windows 2008 is used as RADIUS server.

- Client A
    - MAC address is 0022.0002.0002 and IP address is 1.1.1.2.
    - Client A is configured to use MD5 EAP authentication method with username "vlan200" and a MD5 password.
    - After authentication:
        - Client A should be placed in VLAN 200.
        - Incoming traffic from client A should be filtered by ACL 100.
- Client B
    - MAC address is 0022.0002.0003 and IP is 2.2.2.2.
    - Client B is not 802.1X capable. DUT should use MAC authentication method to authenticate this client.
    - After authentication:
        - Client B should be placed in VLAN 201.
        - Incoming traffic from client B should be filtered by ACL 101.

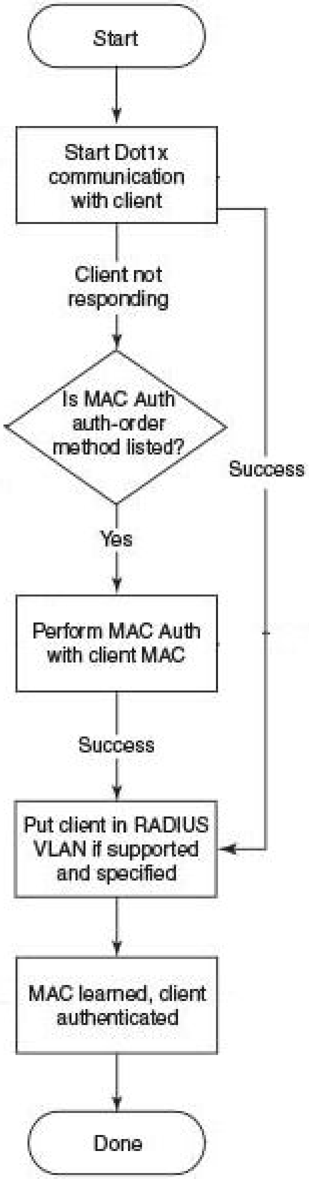
FIGURE 4 Topology A



Flow chart of authentication flow

The switch will follow the flow chart shown in Figure 5 when authenticating client A and client B in this topology.

FIGURE 5 Flow chart of authentication flow in use case 1

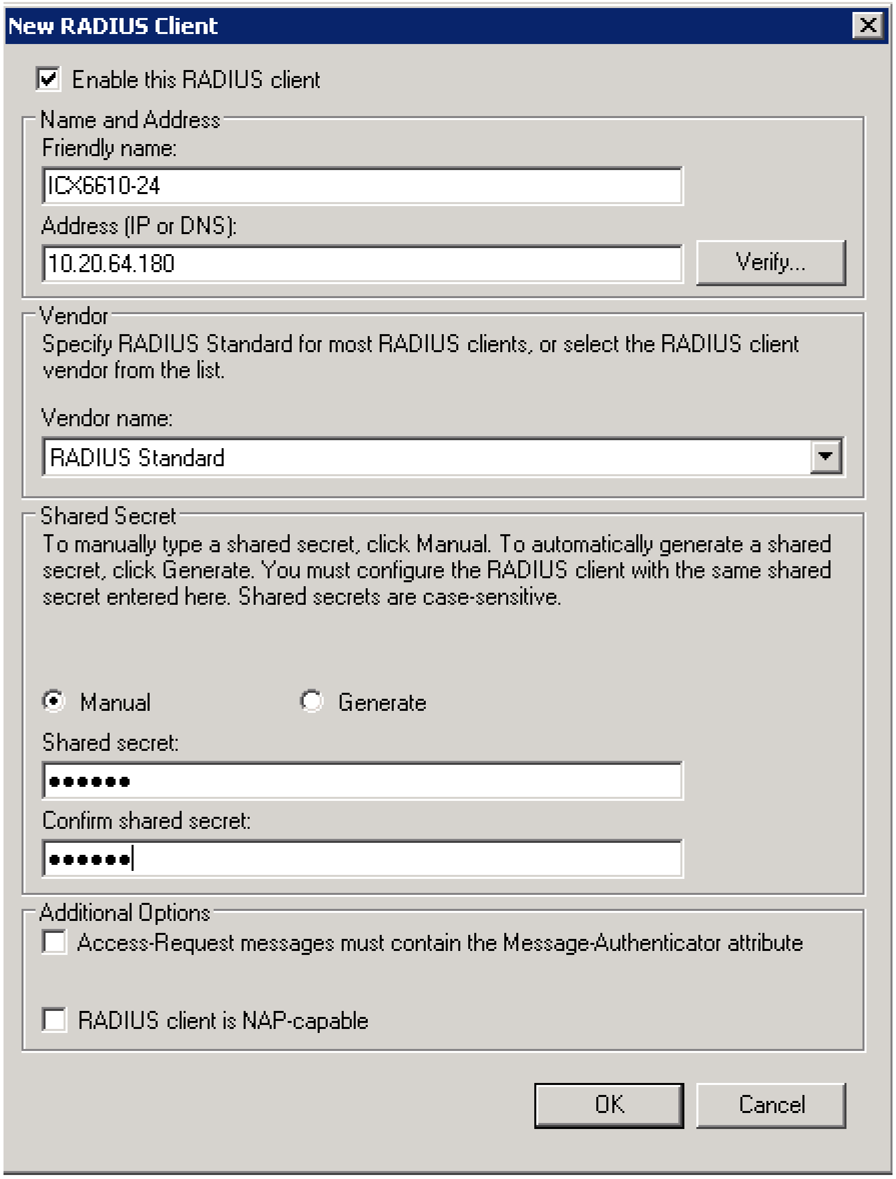

Start
Start Dot1x communication with client
Client not responding
Is MAC Auth auth-order method listed?
Success
Yes
Perform MAC Auth with client MAC
Success
Put client in RADIUS VLAN if supported and specified
MAC learned, client authenticated
Done

Steps to deploy topology A

RADIUS configuration

Step 1: Configure the IP address of the ICX6610-24 switch as a RADIUS client on the RADIUS server. In this example, the IP address of the ICX6610-24 switch is 10.20.64.180. The shared key between the RADIUS server and the ICX6610-24 switch is set to "secret". A screen shot of the "New RADIUS client" configuration window of network policy server is shown in Figure 6 .

FIGURE 6 RADIUS client configuration window



New RADIUS Client

☑ Enable this RADIUS client

Name and Address

Friendly name: ICX6610-24

Address (IP or DNS): 10.20.64.180

Vendor

Specify RADIUS Standard for most RADIUS clients, or select the RADIUS client vendor from the list.

Vendor name: RADIUS Standard

Shared Secret

To manually type a shared secret, click Manual. To automatically generate a shared secret, click Generate. You must configure the RADIUS client with the same shared secret entered here. Shared secrets are case-sensitive.

● Manual ○ Generate

Shared secret: ●●●●●●

Confirm shared secret: ●●●●●●

Additional Options

□ Access-Request messages must contain the Message-Authenticator attribute

□ RADIUS client is NAP-capable

Step 2: Create a connection request policy for user "vlan200" and configure the RADIUS attributes listed in the table below. A screen shot of the RADIUS attribute configuration window of network policy server is given in Figure 7 .

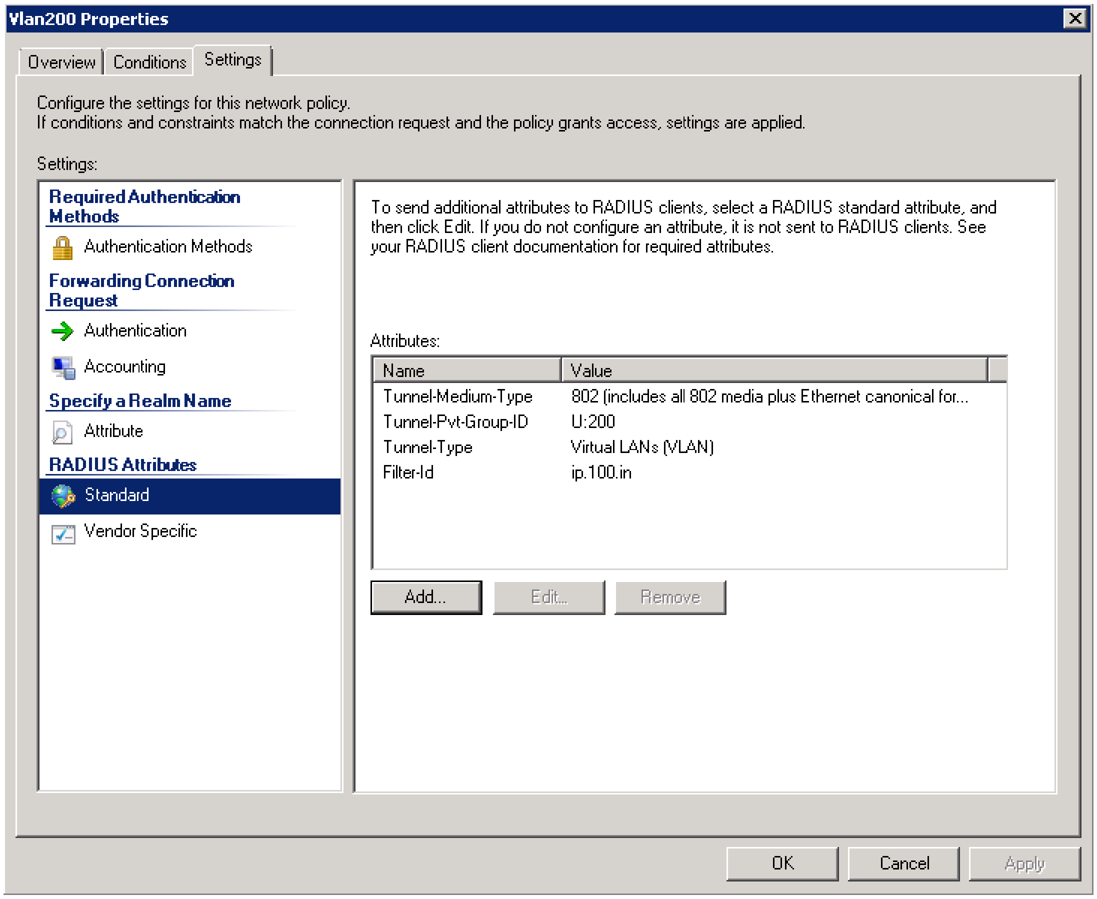
TABLE 1 RADIUS attributes for user "vlan200"

Attribute	Value	Comment
Tunnel-Medium-Type	802	
Tunnel-Pvt-Group-ID	U:200	The format is U:<VLAN-id> It means untagged traffic from this client will be forwarded in this VLAN.
Tunnel-Type	VLAN	

TABLE 1 RADIUS attributes for user "vlan200" (Continued)

Attribute	Value	Comment
Filter-ID	ip.100.in	The format is ip.<ACL-id>.in

FIGURE 7 RADIUS attribute configuration for user "vlan200"



Configure the settings for this network policy.
If conditions and constraints match the connection request and the policy grants access, settings are applied.

To send additional attributes to RADIUS clients, select a RADIUS standard attribute, and then click Edit. If you do not configure an attribute, it is not sent to RADIUS clients. See your RADIUS client documentation for required attributes.

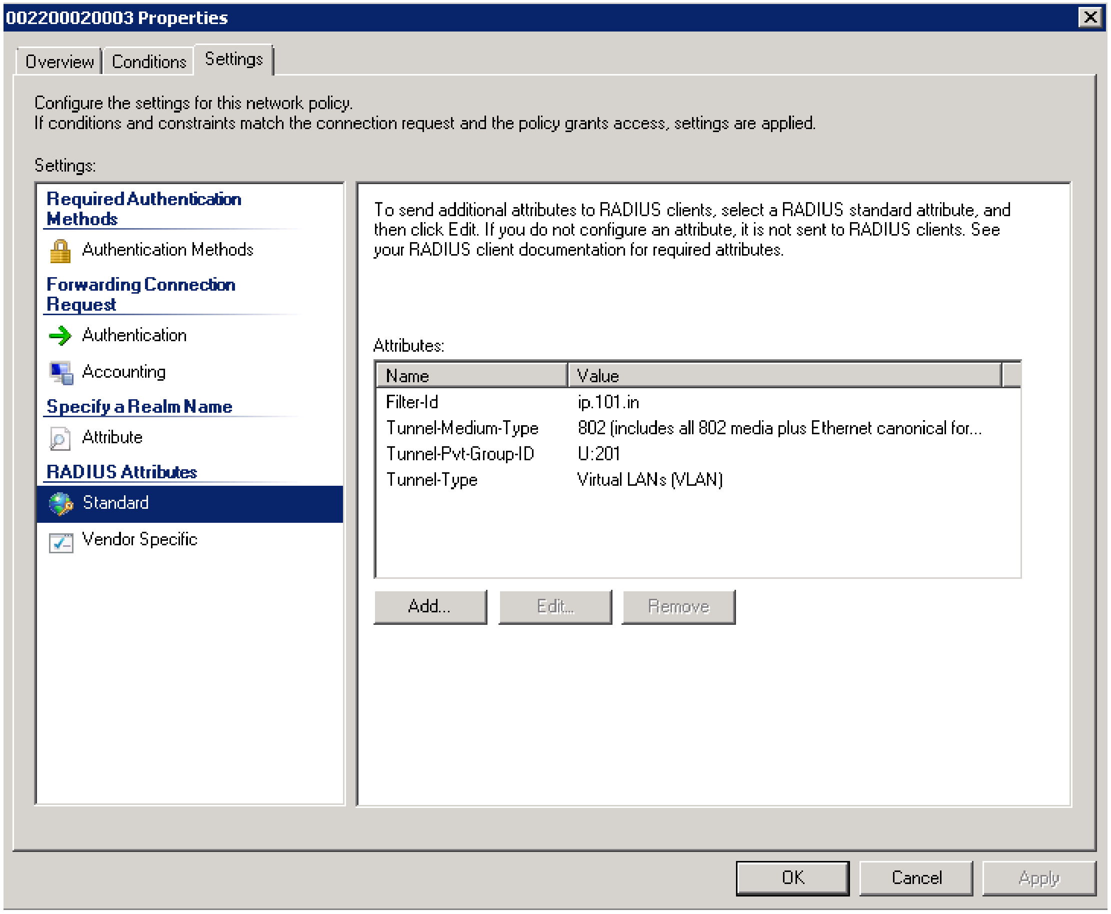
Name	Value
Tunnel-Medium-Type	802 (includes all 802 media plus Ethernet canonical for...
Tunnel-Pvt-Group-ID	U:200
Tunnel-Type	Virtual LANs (VLAN)
Filter-Id	ip.100.in

Step 3: Create a connection request policy for user "002200020003"and configure following RADIUS attributes. A screen shot of the RADIUS attribute configuration window of network policy server is given in Figure 8 .

TABLE 2 RADIUS attributes for user "002200020003"

Attribute	Value	Comment
Tunnel-Medium-Type	802	
Tunnel-Pvt-Group-ID	U:201	The format is U:<VLAN-id> It means untagged traffic from this client will be forwarded in this VLAN.
Tunnel-Type	VLAN	
Filter-ID	ip.100.in	The format is ip.<ACL-id>.in

FIGURE 8 RADIUS attribute configuration for user "002200020003"



002200020003 Properties

Configure the settings for this network policy.
If conditions and constraints match the connection request and the policy grants access, settings are applied.

Settings:

To send additional attributes to RADIUS clients, select a RADIUS standard attribute, and then click Edit. If you do not configure an attribute, it is not sent to RADIUS clients. See your RADIUS client documentation for required attributes.

Attributes:

Name	Value
Filter-Id	ip.101.in
Tunnel-Medium-Type	802 (includes all 802 media plus Ethernet canonical for...
Tunnel-Pvt-Group-ID	U:201
Tunnel-Type	Virtual LANs (VLAN)

Brocade switch configuration

Step 1: Configure an authentication method list for 802.1X and specify RADIUS as an authentication server. Following CLI configures the 802.1X process on the switch to use the configured RADIUS server to authenticate clients.

```
ICX6610-24 Router(config)#aaa authentication dot1x default radius
```

Step 2: Configure a radius server. In this example, radius server's IP address is 10.20.64.208 and shared key is "secret". The shared key should match the key given during client configuration on RADIUS server (refer to section RADIUS configuration on page 12). UDP port 1812 is used for RADIUS authentication messages and UDP port 1813 is used for RADIUS accounting messages.

```
ICX6610-24 Router(config)#radius-server host 10.20.64.208 auth-port 1812 acct-port
1813 default key secret
```

Step 3: Create a VLAN to be used as auth-default-vlan. This VLAN must be configured to enable authentication. When any port is enabled for dot1x or MAC authentication, the port is moved into this VLAN by default as a MAC-based VLAN member. Sometimes the RADIUS server may authenticate the client but not return the required VLAN information on where the client should be placed. The auth-default VLAN is used in this scenario.

```
ICX6610-24 Router(config)#vlan 2 name auth-default-vlan
ICX6610-24 Router(config-vlan-2)#untagged ethernet 1/1/12
```

Step 4: Create the VLANs that will be assigned to clients by RADIUS. RADIUS will return VLAN 200 for Client A and VLAN 201 for Client B, these two VLANs must exist in the Brocade switch. In this example, two VLANS 200 and 201 are created. In addition, virtual interfaces 200 and 201 are also created in these VLANS respectively, so that client A and B can use the virtual interface IP as their gateway IP.

```
ICX6610-24 Router(config)#vlan 200 name clientA
ICX6610-24 Router(config-vlan-200)#untagged ethernet 2/1/12
ICX6610-24 Router(config-vlan-200)#router-interface ve 200
ICX6610-24 Router(config-vlan-200)#exit
ICX6610-24 Router(config)#vlan 201 name clientB
ICX6610-24 Router(config-vlan-201)#untagged ethernet 5/1/12
ICX6610-24 Router(config-vlan-201)#router-interface ve 201
ICX6610-24 Router(config-vlan-201)#exit
ICX6610-24 Router(config)#int ve 200
ICX6610-24 Router(config-vif-200)#ip address 1.1.1.1/24
ICX6610-24 Router(config-vif-200)#exit
ICX6610-24 Router(config)#int ve 201
ICX6610-24 Router(config-vif-201)#ip address 2.2.2.1/24
ICX6610-24 Router(config-vif-201)#exit
```

Step 5: Specify which VLAN ID to use as auth-default-vlan under authentication mode. This VLAN must be configured to enable authentication. When any port is enabled for 802.1X or MAC authentication, the port is moved into this VLAN by default as a MAC-based VLAN member. Sometimes the RADIUS server may authenticate the client but not return the required VLAN information on where the client should be placed. The auth-default VLAN is used in this scenario.

```
ICX6610-24 Router(config)#authentication
ICX6610-24 Router(config-authen)#auth-default-vlan 2
```

Step 6: Enable 802.1X on the switch under authentication mode and enable 802.1X on port 1/1/11. Configure port-control mode as "auto" under interface configuration mode. The mode "auto" enables the 802.1X authentication on the interface.

```
ICX6610-24 Router(config-authen)#dot1x enable
ICX6610-24 Router(config-authen)#dot1x enable ethernet 1/1/11
ICX6610-24 Router(config-authen)#exit
ICX6610-24 Router(config)#interface ethernet 1/1/11
ICX6610-24 Router(config-if-e1000-1/1/11)#dot1x port-control auto
ICX6610-24 Router(config-if-e1000-1/1/11)#exit
```

Step 7: Enable MAC authentication on the switch under authentication mode and enable MAC authentication for port 1/1/11.

```
ICX6610-24 Router(config)#authentication
ICX6610-24 Router(config-authen)#mac-auth enable
ICX6610-24 Router(config-authen)#mac-auth enable ethernet 1/1/11
ICX6610-24 Router(config-authen)#exit
```

Step 8: Configure two ACLs, 100 and 101. These two ACLs must exist in the switch. RADIUS will return ACL 100 for Client A and ACL 101 for client B. The source IP must be "any" as the Brocade switch dynamically learns the IP addresses of the clients (source). The destination network is user configurable. In this example, destination network is set to "any" for simplicity.

```
ICX6610-24 Router(config)#access-list 100 permit ip any any
ICX6610-24 Router(config)#access-list 101 permit ip any any
```

Step 9: Authentication related configurations are stored under the key word "authentication". To verify authentication related configuration on the switch, use CLI "show running-configuration | begin authentication".

```
ICX6610-24 Router#show running-configuration | begin authentication
authentication
 auth-default-vlan 2
 dot1x enable
 dot1x enable ethe 1/1/11
 mac-authentication enable
 mac-authentication enable ethe 1/1/11
!
!
!
```

Client authentication and verification

Step 1: Connect Client A to port 1/1/11 via hub. When ICX6610-24 switch detects the MAC address of Client A on port 1/1/11, it prints a syslog indicating that this MAC address is unauthorized and sends "EAP-Request/Identify". After successful RADIUS authentication, the switch sends "EAP-success" message to the client and prints a syslog indicating that the MAC address of client A is authorized.

Refer to Figure 1 on page 5 for more information regarding messages exchanged between client, switch and RADIUS server.

```
ICX6610-24 Router#
SYSLOG: <14>Oct  7 11:24:58 DOT1X: Port 1/1/11 - mac 0022.0002.0002
AuthControlledPortStatus change: unauthorized

SYSLOG: <14>Oct  7 11:24:59 DOT1X: Port 1/1/11 - mac 0022.0002.0002,
AuthControlledPortStatus change: authorized
```

Step 2: Verify Client A's successful authentication:

- Verify Client A is authenticated using "show dot1x sessions ethernet 1/1/11" and look for the "PAE(Port Access Entity) state".
- Verify port 1/1/11 is part of VLAN 200 using "show vlan 20".
- Verify ACL 100 is applied using "show dot1x ip-acl ethernet 1/1/11".

```
ICX6610-24 Router#
ICX6610-24 Router#show dot1x sessions ethernet 1/1/11
--------------------------------------------------------------------------------------
------

Port        MAC             IP              User         Vlan   Auth       ACL
Age   PAE
            Addr            Addr            Name                State
State
--------------------------------------------------------------------------------------
------
1/1/11   0022.0002.0002  1.1.1.2         vlan200         200  permit  in-100  Ena
AUTHENTICATED
ICX6610-24 Router#
ICX6610-24 Router#show vlan 200
Total PORT-VLAN entries: 22
Maximum PORT-VLAN entries: 4095

Legend: [Stk=Stack-Id, S=Slot]

PORT-VLAN 200, Name clientA, Priority level0, Spanning tree Off
 Untagged Ports: (U2/M1)  12
   Tagged Ports: None
   Uplink Ports: None
 DualMode Ports: None
 Mac-Vlan Ports: (U1/M1)  11
     Monitoring: Disabled

ICX6610-24 Router#
ICX6610-24 Router#show dot1x ip-acl ethernet 1/1/11
802.1X IP ACL Information :
Port 1/1/11 : 0022.0002.0002
In-bound IP ACL : 100
ICX6610-24 Router#
```

Step 3: Ping client A's IP address 1.1.1.2 from the switch to test IP connectivity. As the MAC address of client A is authenticated, ICMP reply from this client will be allowed on port 1/1/11.

```
ICX6610-24 Router#ping 1.1.1.2
Sending 1, 16-byte ICMP Echo to 1.1.1.2, timeout 5000 msec, TTL 64
Type Control-c to abort
Reply from 1.1.1.2         : bytes=16 time=1ms TTL=64
Success rate is 100 percent (1/1), round-trip min/avg/max=1/1/1 ms.
```

Step 4: Connect Client B to port 1/1/11 via hub. When ICX6610-24 switch detects the MAC address of Client B on port 1/1/11, it prints a syslog indicating that this MAC address is unauthorized and sends "EAP-Request/Identify". When the switch does not receive "EAP-response" from client B within 60 seconds, 802.1X process times out, and MAC authentication is attempted for this client using MAC address as username and password. After successful RADIUS authentication, the switch prints a syslog indicating that MAC authentication succeeded for client B's MAC address.

```
ICX6610-24 Router#
SYSLOG: <14>Oct  7 11:57:59 DOT1X: Port 1/1/11 - mac 0022.0002.0003
AuthControlledPortStatus change:
unauthorized

SYSLOG: <13>Oct  7 11:58:59 MAC Authentication succeeded for [0022.0002.0003 ] on
port 1/1/11
```

Step 5: Verify Client B's successful authentication:

- Verify Client B is authenticated using "show mac-auth sessions ethernet 1/1/11" and look for the "Auth State".
- Verify port 1/1/11 is part of VLAN 201 using "show vlan 201".
- Verify ACL 101 is applied using "show mac-auth ip-acl ethernet 1/1/11".

```
ICX6610-24 Router#
ICX6610-24 Router#
ICX6610-24 Router#show mac-auth sessions ethernet 1/1/11
------------------------------------------------------------------------------

Port    MAC            IP               Vlan   Auth        ACL    Age
        Addr           Addr                    State
------------------------------------------------------------------------------
1/1/11   0022.0002.0003  2.2.2.2         201  Yes     in-101  Ena
ICX6610-24 Router#
ICX6610-24 Router#
ICX6610-24 Router#show vlan 201
Total PORT-VLAN entries: 22
Maximum PORT-VLAN entries: 4095

Legend: [Stk=Stack-Id, S=Slot]

PORT-VLAN 201, Name clientB, Priority level0, Spanning tree Off
 Untagged Ports: (U5/M1)  12
   Tagged Ports: None
   Uplink Ports: None
 DualMode Ports: None
 Mac-Vlan Ports: (U1/M1)  11
     Monitoring: Disabled

ICX6610-24 Router#
ICX6610-24 Router#
ICX6610-24 Router#show mac-auth ip-acl ethernet 1/1/11
MAC-Auth IP ACL Information :
Port 1/1/11 : 0022.0002.0003
In-bound IP ACL : 101
ICX6610-24 Router#
```

Step 6: Ping client B's IP address 2.2.2.2 from the switch to test IP connectivity. As the MAC address of client B is authenticated, ICMP reply from this client will be allowed on port 1/1/11.

```
ICX6610-24 Router#ping 2.2.2.2
Sending 1, 16-byte ICMP Echo to 2.2.2.2, timeout 5000 msec, TTL 64
Type Control-c to abort
Reply from 2.2.2.2           : bytes=16 time=1ms TTL=64
Success rate is 100 percent (1/1), round-trip min/avg/max=1/1/1 ms.
```

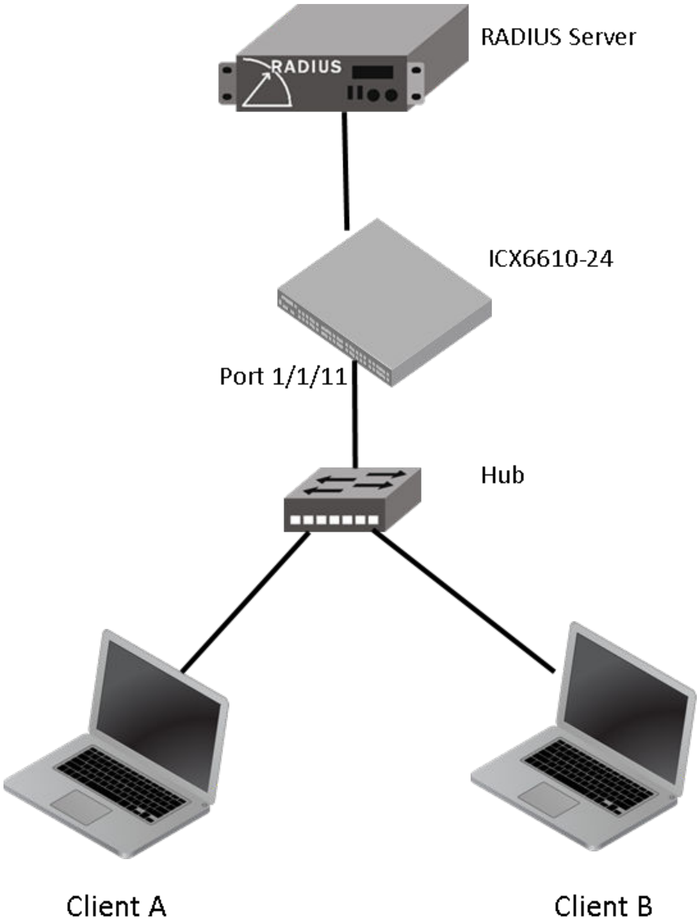
Use Case 2: Dynamic VLAN and ACL assignment with authentication order - MAC authentication followed by 802.1X

This use case demonstrates the capability of a Brocade switch to maintain different network policies for each client connected to the same port. The flexible authentication order is set to MAC authentication followed by 802.1X. In topology B, there are two clients (Client A and Client B) connected to port 1/1/11 of an ICX6610-24 via hub. The hub is used to connect two clients to the same port. ICX6610-24 has IP connectivity to the RADIUS server. The server's IP address is 10.20.64.208. In this topology, network policy server on a PC running windows 2008 is used as RADIUS server.

- Client A:
  - MAC address is 0022.0002.0002 and IP address is 1.1.1.2
  - Client A is configured to use MD5 EAP authentication method with username "vlan200" and a MD5 password.
  - DUT should attempt both MAC-authentication and 802.1X authentication.
  - After both authentication methods succeed

  - Client A should be placed in VLAN 200.
  - Incoming traffic from client A should be filtered by ACL 100.
- Client B:
  - MAC address is 0022.0002.0003 and IP is 2.2.2.2.
  - Client B is not 802.1X capable.
  - DUT should only use MAC authentication method to authenticate this client.
  - After authentication
    - Client B should be placed in VLAN 201.
    - Incoming traffic from client B should be filtered by ACL 101.

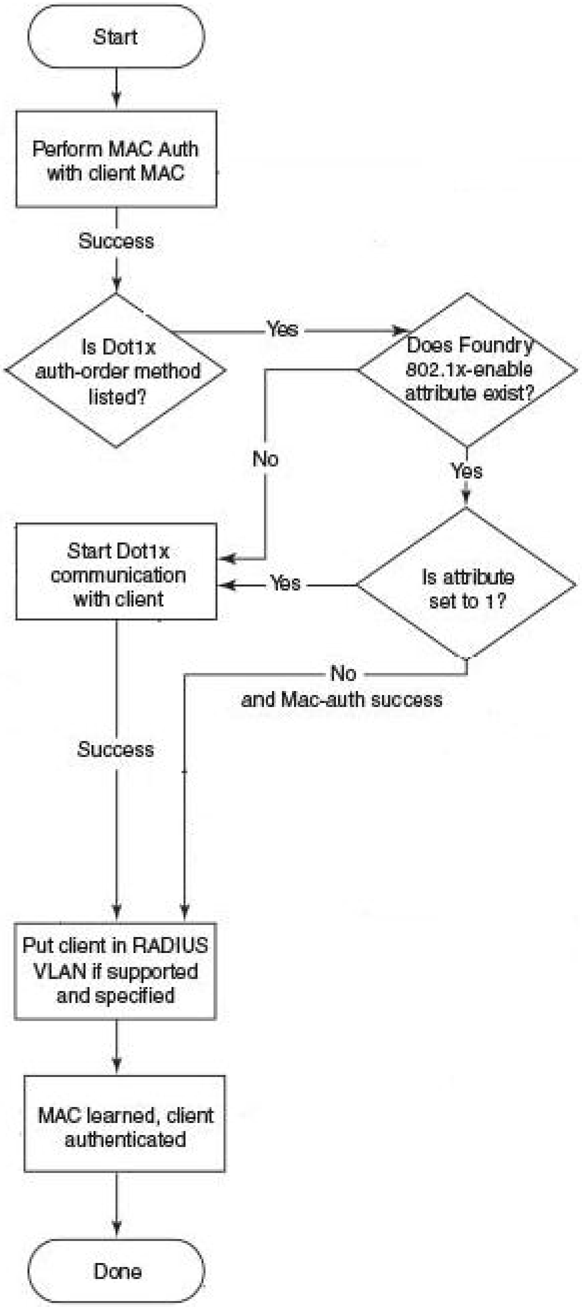
FIGURE 9 Topology B



Flow chart of authentication flow

The switch will follow the flow chart shown in Figure 10 when authenticating client A and client B in this topology.

FIGURE 10 Flowchart of authentication flow in use case 2

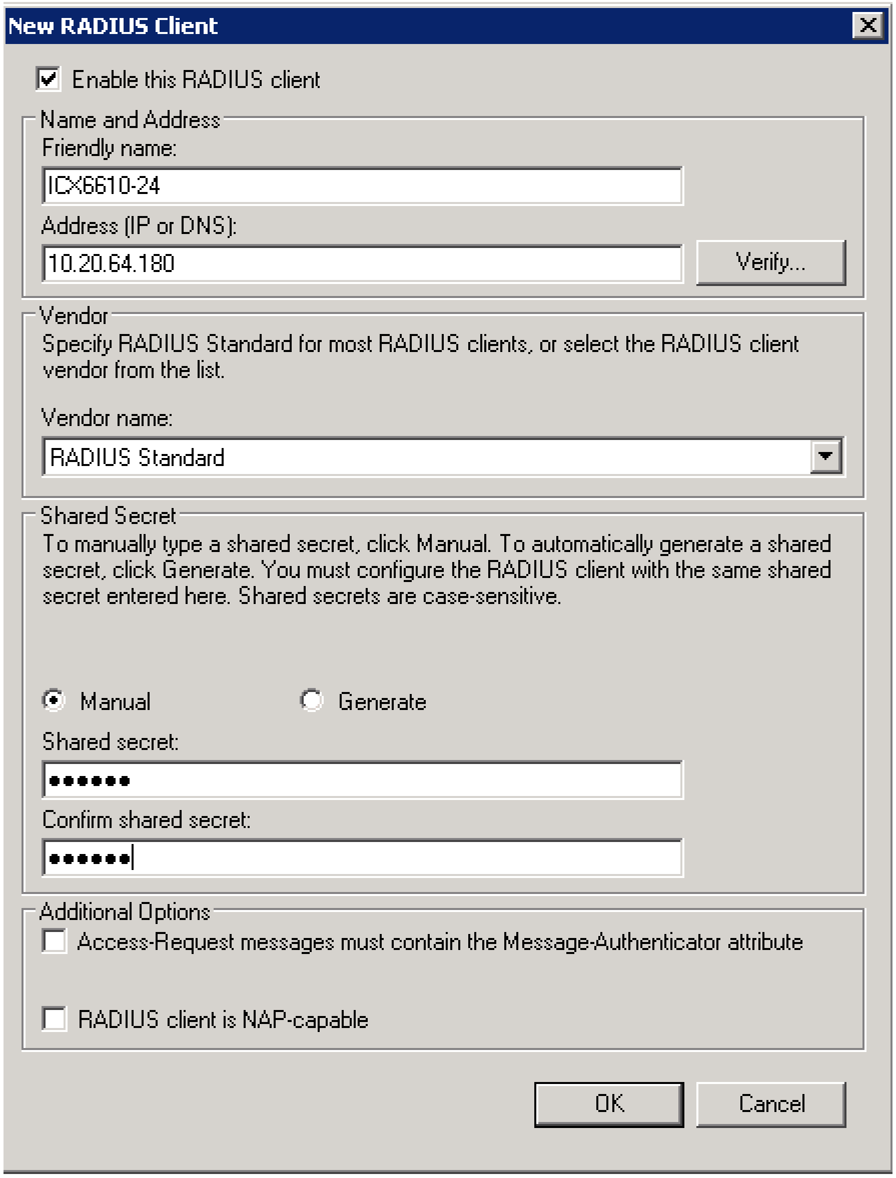

Start
Perform MAC Auth with client MAC
Success
Is Dot1x auth-order method listed?
Yes
Does Foundry 802.1x-enable attribute exist?
No
Yes
Start Dot1x communication with client
Yes
Is attribute set to 1?
No and Mac-auth success
Success
Put client in RADIUS VLAN if supported and specified
MAC learned, client authenticated
Done

Steps to deploy topology B

RADIUS configuration

Step 1: Configure ICX6610-24 switch's IP address as a RADIUS client on the RADIUS server. In this example, ICX6610-24 switch's IP address is 10.20.64.180 and shared key between RADIUS server and ICX6610-24 switch is set to "secret". A screen shot of the "New RADIUS client" configuration window of network policy server is shown in Figure 11 .

FIGURE 11 RADIUS client configuration window



New RADIUS Client

☑ Enable this RADIUS client

Name and Address

Friendly name: ICX6610-24

Address (IP or DNS): 10.20.64.180

Vendor

Specify RADIUS Standard for most RADIUS clients, or select the RADIUS client vendor from the list.

Vendor name: RADIUS Standard

Shared Secret

To manually type a shared secret, click Manual. To automatically generate a shared secret, click Generate. You must configure the RADIUS client with the same shared secret entered here. Shared secrets are case-sensitive.

● Manual ○ Generate

Shared secret: ●●●●●●

Confirm shared secret: ●●●●●●

Additional Options

□ Access-Request messages must contain the Message-Authenticator attribute

□ RADIUS client is NAP-capable

Step 2: Create a connection request policy for user "002200020002" and configure following RADIUS attributes. A screen shot of the RADIUS attribute configuration window of network policy server is given in Figure 12 .

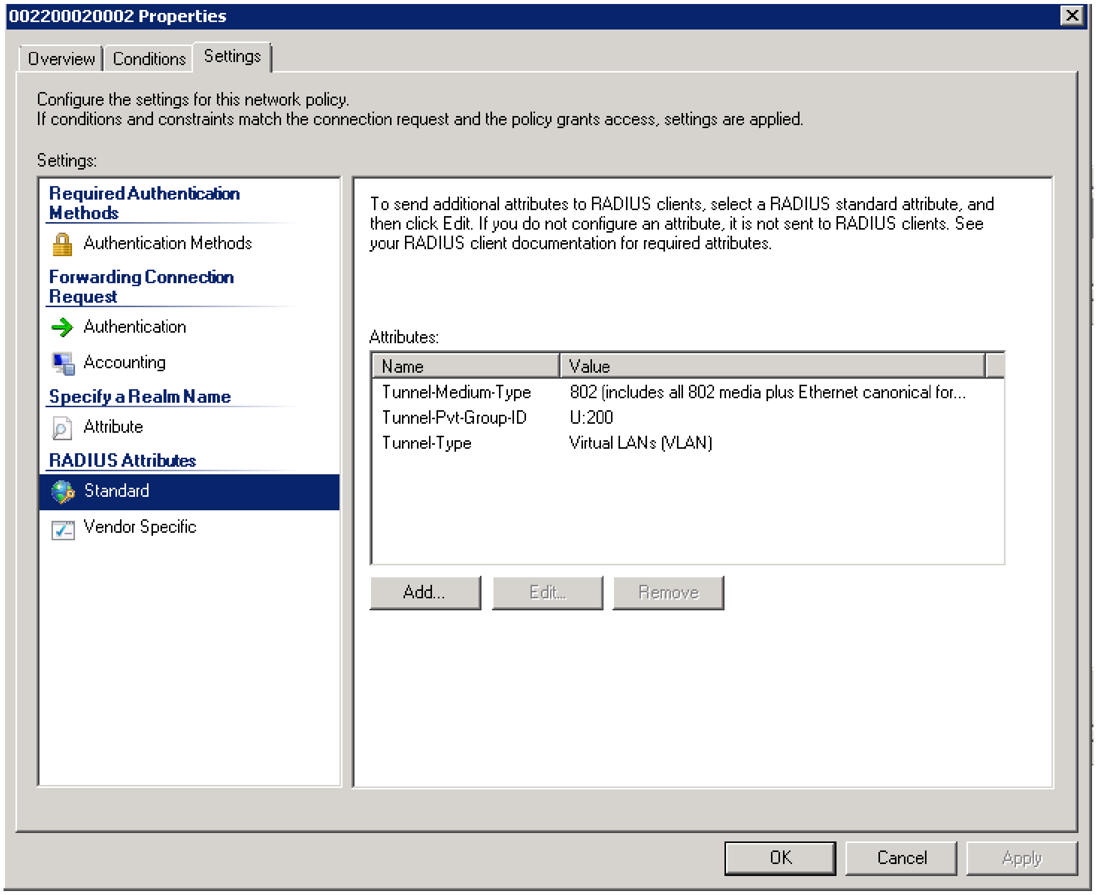
TABLE 3 RADIUS attributes for user "002200020002"

Attribute	Value	Comment
Tunnel-Medium-Type	802	

TABLE 3 RADIUS attributes for user "002200020002" (Continued)

Attribute	Value	Comment
Tunnel-Pvt-Group-ID	U:200	The format is U:<VLAN-id> It means untagged traffic from this client will be forwarded in this VLAN
Tunnel-Type	VLAN	

FIGURE 12 RADIUS attribute configuration for user "002200020002"



Configure the settings for this network policy.
If conditions and constraints match the connection request and the policy grants access, settings are applied.

To send additional attributes to RADIUS clients, select a RADIUS standard attribute, and then click Edit. If you do not configure an attribute, it is not sent to RADIUS clients. See your RADIUS client documentation for required attributes.

Attributes:

Name	Value
Tunnel-Medium-Type	802 (includes all 802 media plus Ethernet canonical for...
Tunnel-Pvt-Group-ID	U:200
Tunnel-Type	Virtual LANs (VLAN)

Step 3: Create a connection request policy for user "vlan200" and configure following RADIUS attributes. A screen shot of the RADIUS attribute configuration window of network policy server is given in Figure 13 .

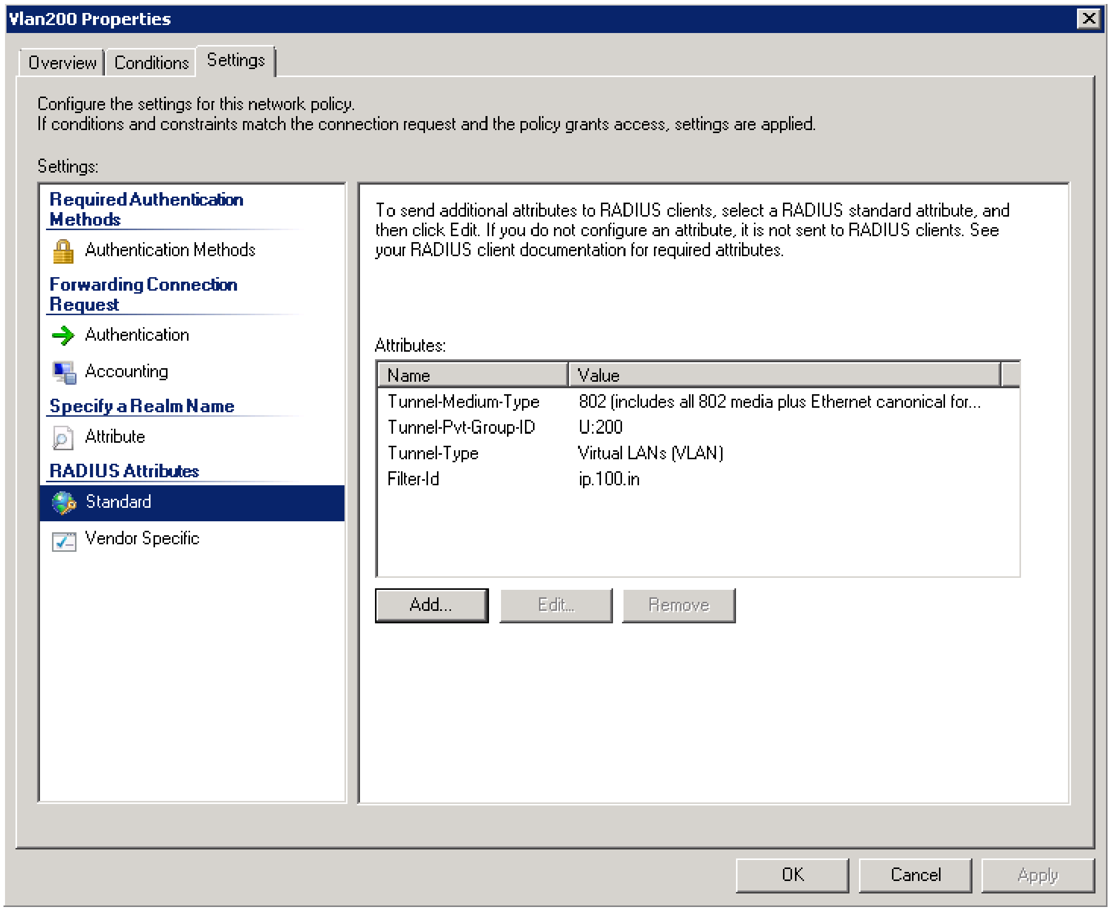
TABLE 4 RADIUS attributes for user "vlan200"

Attribute	Value	Comment
Tunnel-Medium-Type	802	
Tunnel-Pvt-Group-ID	U:200	The format is U:<VLAN-id> It means untagged traffic from this client will be forwarded in this VLAN.
Tunnel-Type	VLAN	

TABLE 4 RADIUS attributes for user "vlan200" (Continued)

Attribute	Value	Comment
Filter-ID	ip.100.in	The format is ip.<ACL-id>.in

FIGURE 13 RADIUS attribute configuration for user "vlan200"



Configure the settings for this network policy.
If conditions and constraints match the connection request and the policy grants access, settings are applied.

To send additional attributes to RADIUS clients, select a RADIUS standard attribute, and then click Edit. If you do not configure an attribute, it is not sent to RADIUS clients. See your RADIUS client documentation for required attributes.

Name	Value
Tunnel-Medium-Type	802 (includes all 802 media plus Ethernet canonical for...
Tunnel-Pvt-Group-ID	U:200
Tunnel-Type	Virtual LANs (VLAN)
Filter-Id	ip.100.in

Step 4: Create a connection request policy for user "002200020003" and configure following RADIUS attributes. Screen shots of the standard RADIUS attribute and vendor specific RADIUS attribute configuration window of network policy server are given in Figure 14 and Figure 15 respectively.

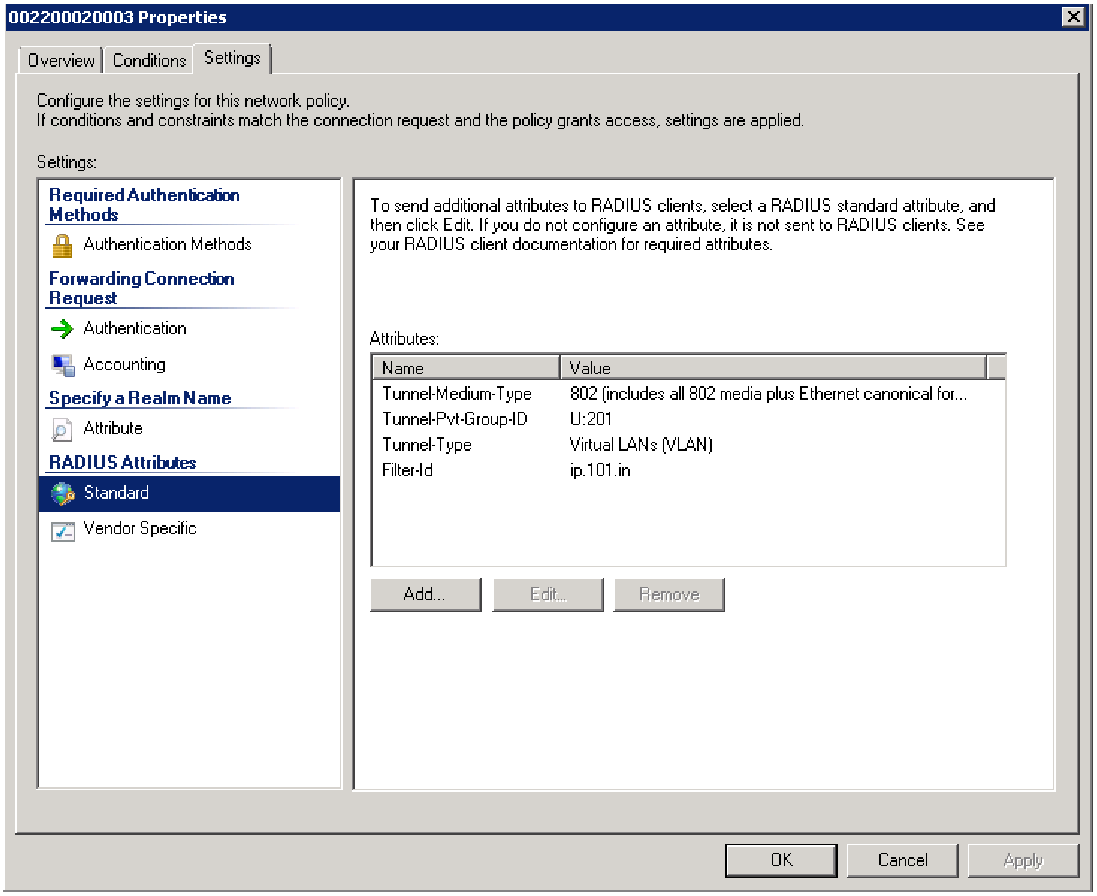
TABLE 5 RADIUS attributes for user "002200020003"

Attribute	Value	Comment
Tunnel-Medium-Type	802	
Tunnel-Pvt-Group-ID	U:200	The format is U:<VLAN-id> It means untagged traffic from this client will be forwarded in this VLAN.
Tunnel-Type	VLAN	
Filter-ID	ip.100.in	The format is ip.<ACL-id>.in

TABLE 5 RADIUS attributes for user "002200020003" (Continued)

Attribute	Value	Comment
Foundry-802_1x-enable (Vendor assigned attribute number 6)	0	If the value is 0, Brocade switch will not attempt 802.1X for this client. If the value is 1 or this attribute is not present in access-accept message, switch will attempt 802.1X for this client

FIGURE 14 Standard RADIUS attribute configuration for user "002200020003"



002200020003 Properties

Configure the settings for this network policy.
If conditions and constraints match the connection request and the policy grants access, settings are applied.

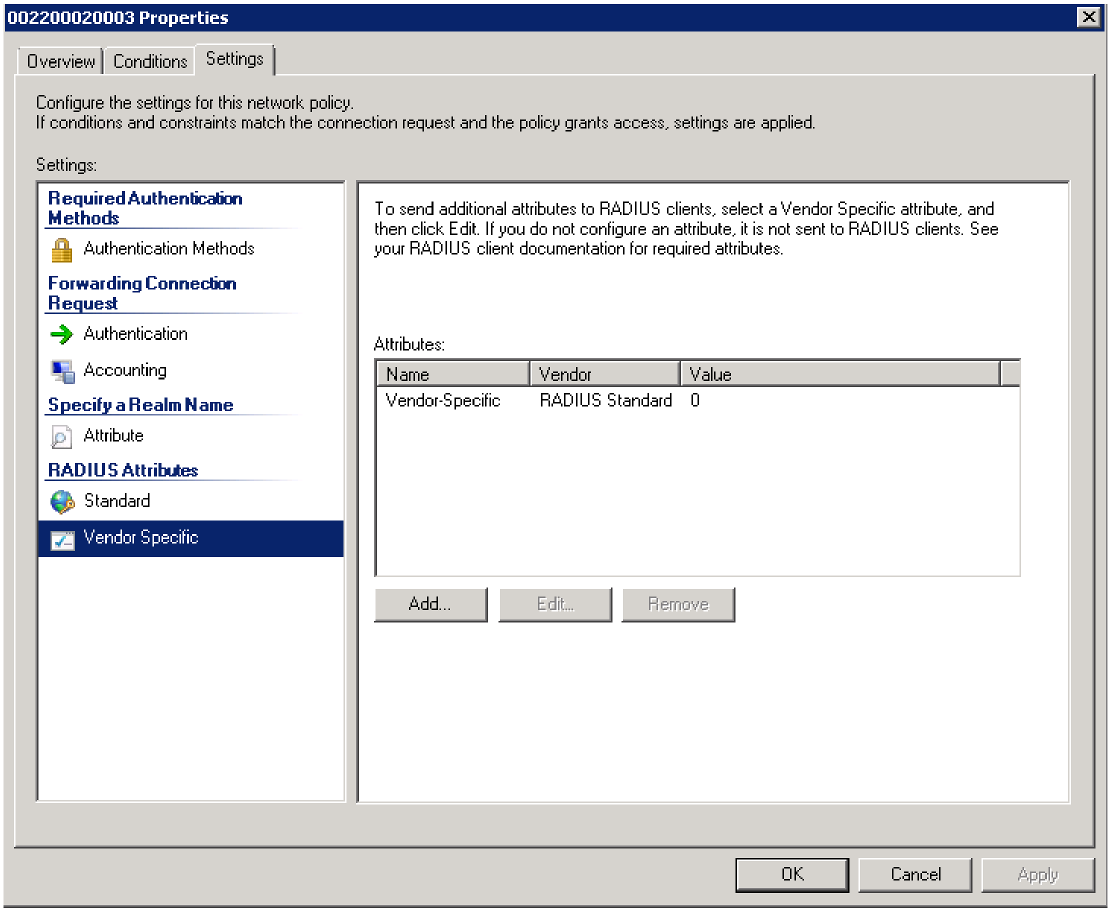
Settings:

To send additional attributes to RADIUS clients, select a RADIUS standard attribute, and then click Edit. If you do not configure an attribute, it is not sent to RADIUS clients. See your RADIUS client documentation for required attributes.

Attributes:

Name	Value
Tunnel-Medium-Type	802 (includes all 802 media plus Ethernet canonical for...
Tunnel-Pvt-Group-ID	U:201
Tunnel-Type	Virtual LANs (VLAN)
Filter-Id	ip.101.in

FIGURE 15 Vendor specific RADIUS attribute configuration for user "002200020003"



Configure the settings for this network policy.
If conditions and constraints match the connection request and the policy grants access, settings are applied.

Settings:

To send additional attributes to RADIUS clients, select a Vendor Specific attribute, and then click Edit. If you do not configure an attribute, it is not sent to RADIUS clients. See your RADIUS client documentation for required attributes.

Attributes:

Name	Vendor	Value
Vendor-Specific	RADIUS Standard	0

Brocade switch configuration

Step 1: Configure an authentication method list for 802.1X and specify RADIUS as an authentication server. Following CLI configures the 802.1X process on the switch to use the configured RADIUS server to authenticate clients.

```
ICX6610-24 Router(config)#aaa authentication dot1x default radius
```

Step 2: Configure a radius server. In this example, radius server's IP address is 10.20.64.208 and shared key is "secret". The shared key should match the key given during client configuration on RADIUS server. UDP port 1812 is used for RADIUS authentication messages and UDP port 1813 is used for RADIUS accounting messages.

```
ICX6610-24 Router(config)#radius-server host 10.20.64.208 auth-port 1812 acct-port
1813 default key secret
```

Step 3: Create a VLAN to be used as auth-default-vlan. This VLAN must be configured to enable authentication. When any port is enabled for dot1x or MAC authentication, the port is moved into this VLAN by default as a MAC-based VLAN member. Sometimes the RADIUS server may authenticate the client but not return the required VLAN information on where the client should be placed. The auth-default VLAN is used in this scenario.

```
ICX6610-24 Router(config)#vlan 2 name auth-default-vlan
ICX6610-24 Router(config-vlan-2)#untagged ethernet 1/1/12
```

Step 4: Create the VLANs that will be assigned to clients by RADIUS. RADIUS will return VLAN 200 for Client A and VLAN 201 for Client B, these two VLANs must exist in the Brocade switch. In this example, two VLANS 200 and 201 are created. In addition, virtual interfaces 200 and 201 are also created in these VLANS respectively, so that client A and B can use the virtual interface IP as their gateway IP.

```
ICX6610-24 Router(config)#vlan 200 name clientA
ICX6610-24 Router(config-vlan-200)#untagged ethernet 2/1/12
ICX6610-24 Router(config-vlan-200)#router-interface ve 200
ICX6610-24 Router(config-vlan-200)#exit
ICX6610-24 Router(config)#vlan 201 name clientB
ICX6610-24 Router(config-vlan-201)#untagged ethernet 5/1/12
ICX6610-24 Router(config-vlan-201)#router-interface ve 201
ICX6610-24 Router(config-vlan-201)#exit
ICX6610-24 Router(config)#int ve 200
ICX6610-24 Router(config-vif-200)#ip address 1.1.1.1/24
ICX6610-24 Router(config-vif-200)#exit
ICX6610-24 Router(config)#int ve 201
ICX6610-24 Router(config-vif-201)#ip address 2.2.2.1/24
ICX6610-24 Router(config-vif-201)#exit
```

Step 5: Specify which VLAN ID to use as auth-default-vlan under authentication mode. This VLAN must be configured to enable authentication. When any port is enabled for 802.1X or MAC authentication, the port is moved into this VLAN by default as a MAC-based VLAN member. Sometimes the RADIUS server may authenticate the client but not return the required VLAN information on where the client should be placed. The auth-default VLAN is used in this scenario.

```
ICX6610-24 Router(config)#authentication
ICX6610-24 Router(config-authen)#auth-default-vlan 2
```

Step 6: Configure authentication order to be MAC authentication followed by 802.1X under authentication mode.

```
ICX6610-24 Router(config)#authentication
ICX6610-24 Router(config-authen)#auth-order mac-auth dot1x
```

Step 7: Enable 802.1X on the switch under authentication mode and enable 802.1X on port 1/1/11. Configure port-control mode as "auto" under interface configuration mode. The mode "auto" enables the 802.1X authentication on the interface.

```
ICX6610-24 Router(config)#authentication
ICX6610-24 Router(config-authen)#dot1x enable
ICX6610-24 Router(config-authen)#dot1x enable ethernet 1/1/11
ICX6610-24 Router(config-authen)#exit
ICX6610-24 Router(config)#interface ethernet 1/1/11
ICX6610-24 Router(config-if-e1000-1/1/11)#dot1x port-control auto
ICX6610-24 Router(config-if-e1000-1/1/11)#exit
```

Step 8: Enable MAC authentication on the switch under authentication mode and enable MAC authentication for port 1/1/11.

```
ICX6610-24 Router(config)#authentication
ICX6610-24 Router(config-authen)#mac-auth enable
ICX6610-24 Router(config-authen)#mac-auth enable ethernet 1/1/11
ICX6610-24 Router(config-authen)#exit
```

Step 9: RADIUS will return ACL 100 for Client A and ACL 101 for client B. These two ACLs must exist in the switch. The source IP must be "any" as the Brocade switch dynamically learns the IP addresses of the clients (source). The destination network is user configurable. In this example, destination network is set to "any" for simplicity.

```
ICX6610-24 Router(config)#access-list 100 permit ip any any
ICX6610-24 Router(config)#access-list 101 permit ip any any
```

Step 10: Authentication related configurations are stored under the key word "authentication". To verify authentication related configuration on the switch, use CLI "show running-configuration | begin authentication".

```
ICX6610-24 Router#show running-configuration | begin authentication
authentication
 auth-order mac-auth dot1x
 auth-default-vlan 2
 dot1x enable
 dot1x enable ethe 1/1/11
 mac-authentication enable
 mac-authentication enable ethe 1/1/11
!
!
!
```

Client authentication and verification

Step 1: Connect Client A to port 1/1/11 via hub. When ICX6610-24 switch detects the MAC address of Client A on port 1/1/11, it prints a syslog indicating that this MAC address is unauthorized. MAC authentication is attempted for this client using MAC address as username and password. After successful RADIUS authentication, the switch prints a syslog indicating that MAC authentication succeeded for client A's MAC address. Switch sends "EAP-Request/Identify". After successful RADIUS authentication for 802.1X process, the switch sends "EAP-success" message to the client and prints another syslog indicating that the MAC address of client A is authorized by 802.1X process. Refer Figure 1 on page 5 for more information regarding messages exchanged between client, switch and RADIUS server during 802.1X process.

```
ICX6610-24 Router#
SYSLOG: <14>Oct  7 16:52:16 DOT1X: Port 1/1/11 - mac 0022.0002.0002
AuthControlledPortStatus change:
unauthorized

SYSLOG: <13>Oct  7 16:52:16 MAC Authentication succeeded for [0022.0002.0002 ] on
port 1/1/11

SYSLOG: <14>Oct  7 16:52:16 DOT1X: Port 1/1/11 - mac 0022.0002.0002,
AuthControlledPortStatus change:
authorized
```

Step 2: Verification of Client A's successful authentication:

- Verify Client A is MAC authenticated using "show mac-auth sessions ethernet 1/1/11" and look for "Auth State".
- Verify Client A is 802.1X authenticated using "show dot1x sessions ethernet 1/1/11" and look for "PAE (Port Access Entity) state".
- Verify port 1/1/11 is part of VLAN 200 using "show vlan 200".
- Verify ACL 100 is applied using "show dot1x ip-acl ethernet 1/1/11".

```
ICX6610-24 Router#show mac-auth sessions ethernet 1/1/11
------------------------------------------------------------------------------

Port    MAC            IP               Vlan   Auth        ACL    Age
        Addr           Addr                    State
------------------------------------------------------------------------------
1/1/11   0022.0002.0002  1.1.1.2         200  Yes     none     Ena
ICX6610-24 Router#
ICX6610-24 Router#
ICX6610-24 Router#show dot1x sessions ethernet 1/1/11
---------------------------------------------------------------------------------------
------

Port        MAC             IP              User          Vlan   Auth       ACL
Age   PAE
            Addr            Addr            Name                 State
State
---------------------------------------------------------------------------------------
------
1/1/11   0022.0002.0002  1.1.1.2         vlan200          200  permit  in-100  Ena
AUTHENTICATED
ICX6610-24 Router#
ICX6610-24 Router#show vlan 200
Total PORT-VLAN entries: 22
Maximum PORT-VLAN entries: 4095

Legend: [Stk=Stack-Id, S=Slot]

PORT-VLAN 200, Name clientA, Priority level0, Spanning tree Off
 Untagged Ports: (U2/M1)  12
   Tagged Ports: None
   Uplink Ports: None
 DualMode Ports: None
 Mac-Vlan Ports: (U1/M1)  11
     Monitoring: Disabled

ICX6610-24 Router#
ICX6610-24 Router#show dot1x ip-acl ethernet 1/1/11
802.1X IP ACL Information :
Port 1/1/11 : 0022.0002.0002
```

```
In-bound IP ACL : 100
ICX6610-24 Router#
```

Step 3: Ping client A's IP address 1.1.1.2 from the switch to test IP connectivity. As the MAC address of client A is authenticated, ICMP reply from this client will be allowed on port 1/1/11.

```
ICX6610-24 Router#ping 1.1.1.2
Sending 1, 16-byte ICMP Echo to 1.1.1.2, timeout 5000 msec, TTL 64
Type Control-c to abort
Reply from 1.1.1.2         : bytes=16 time=1ms TTL=64
Success rate is 100 percent (1/1), round-trip min/avg/max=1/1/1 ms.
```

Step 4: Connect Client B to port 1/1/11 via hub. When ICX6610-24 switch detects the MAC address of Client B on port 1/1/11, MAC authentication is attempted for this client using MAC address as username and password. After successful RADIUS authentication, the switch prints a syslog indicating that MAC authentication succeeded for client B's MAC address. And 802.1X method is skipped due to "Foundry-802_1x-enable" attribute value 0 from RADIUS. Notice that a syslog was not generated by the 802.1X process indicating 802.1X process was attempted.

```
ICX6610-24 Router#
SYSLOG: <13>Oct  7 16:55:56 MAC Authentication succeeded for [0022.0002.0003 ] on
port 1/1/11
```

Step 5: Verification of Client B's successful authentication:

- Verify Client B is MAC authenticated using "show mac-auth sessions ethernet 1/1/11" and look for "Auth State."
- Verify port 1/1/11 is part of VLAN 201 using "show vlan 201".
- Verify ACL 101 is applied using "show mac-auth ip-acl ethernet 1/1/11".

```
ICX6610-24 Router#
ICX6610-24 Router#
ICX6610-24 Router#show mac-auth sessions ethernet 1/1/11
-----------------------------------------------------------------------------

Port    MAC            IP              Vlan   Auth        ACL    Age
        Addr           Addr                   State
-----------------------------------------------------------------------------
1/1/11   0022.0002.0003  2.2.2.2         201  Yes     in-101  Ena
ICX6610-24 Router#
ICX6610-24 Router#
ICX6610-24 Router#show vlan 201
Total PORT-VLAN entries: 22
Maximum PORT-VLAN entries: 4095

Legend: [Stk=Stack-Id, S=Slot]

PORT-VLAN 201, Name clientB, Priority level0, Spanning tree Off
 Untagged Ports: (U5/M1)  12
   Tagged Ports: None
   Uplink Ports: None
 DualMode Ports: None
 Mac-Vlan Ports: (U1/M1)  11
     Monitoring: Disabled

ICX6610-24 Router#
ICX6610-24 Router#
ICX6610-24 Router#show mac-auth ip-acl ethernet 1/1/11
MAC-Auth IP ACL Information :
Port 1/1/11 : 0022.0002.0003
In-bound IP ACL : 101
ICX6610-24 Router#
ICX6610-24 Router#
```

Step 6: Ping client B's IP address 2.2.2.2 from the switch to test IP connectivity. As the MAC address of client B is authenticated, ICMP reply from this client will be allowed on port 1/1/11.

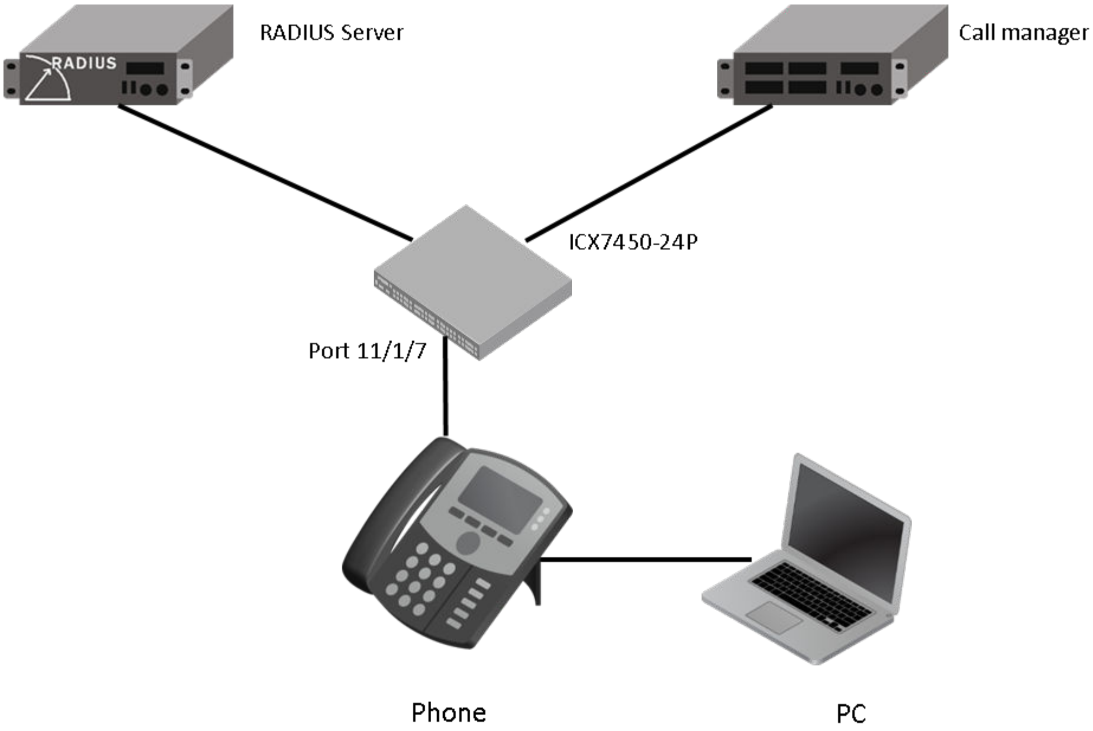
```
ICX6610-24 Router#ping 2.2.2.2
Sending 1, 16-byte ICMP Echo to 2.2.2.2, timeout 5000 msec, TTL 64
Type Control-c to abort
Reply from 2.2.2.2         : bytes=16 time=1ms TTL=64
Success rate is 100 percent (1/1), round-trip min/avg/max=1/1/1 ms.
```

Use Case 3: Authenticating a 802.1X Phone and a PC on the same port

This is probably the most common deployment for an IP phone and a PC. In this topology, we have an 802.1X capable Cisco 7965G IP phone and a PC connected to port 11/1/7 of an ICX7450-24P switch. The flexible authentication order is set to default (802.1X followed by MAC authentication). The ICX7450-24P switch has IP connectivity to the RADIUS server. The server's IP address is 10.20.64.208. In this topology, network policy server on a PC running windows 2008 is used as RADIUS server. The call manager's IP address is 10.20.74.31.

- Cisco 7965G IP Phone:
  - MAC address is 0024.C442.BB24.
  - Phone is configured to use MD5 EAP authentication method with username "CP-7965G-SEP0024C442BB24" and a MD5 password.
  - After 802.1X authentication, the phone should be placed in both data VLAN 200 and voice VLAN 201.
- PC:
  - MAC address is 0022.0002.0002 and IP is 10.20.74.2.
  - PC is configured to use MD5 EAP authentication method with username "vlan200" and a MD5 password.
  - After 802.1X authentication, the PC should be placed in data VLAN 200.

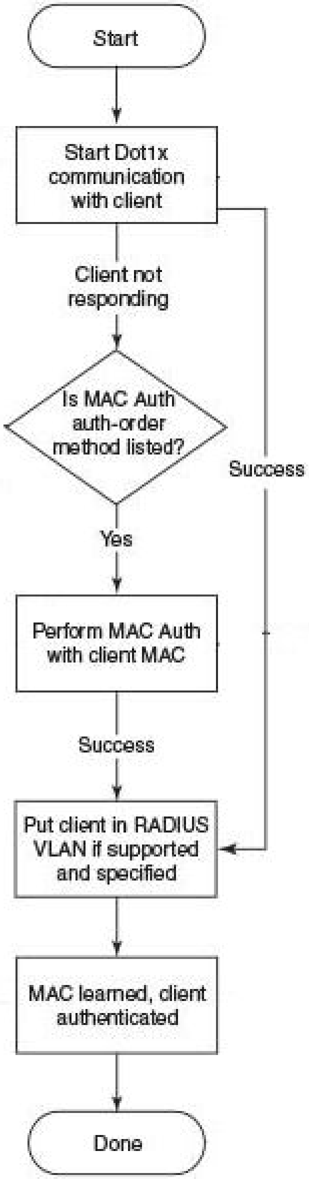
FIGURE 16 Topology C



Flow chart of authentication flow

The switch will follow the flow chart shown in Figure 17 when authenticating Phone and PC in this topology.

FIGURE 17 Flowchart of authentication flow in use case 3

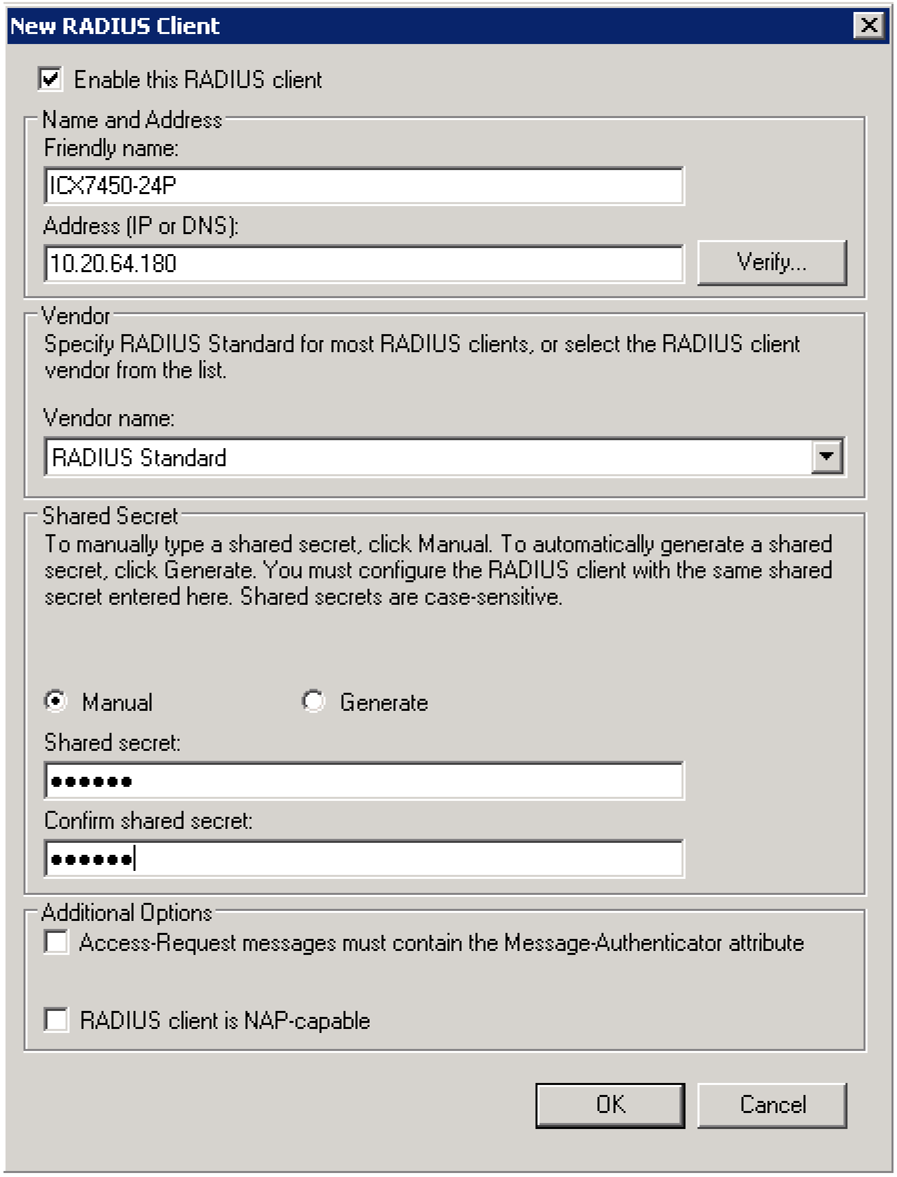

Start
Start Dot1x communication with client
Client not responding
Is MAC Auth auth-order method listed?
Success
Yes
Perform MAC Auth with client MAC
Success
Put client in RADIUS VLAN if supported and specified
MAC learned, client authenticated
Done

Steps to deploy Authentication for a 802.1X Phone and a PC on the same port

RADIUS configuration

Step 1: Configure ICX7450-24P switch's IP address as a RADIUS client on the RADIUS server. In this example, ICX7450-48P switch's IP address is 10.20.64.180 and shared key between RADIUS server and ICX6610-24 switch is set to "secret". A screen shot of the "New RADIUS client" configuration window of network policy server is shown in Figure 18 .

FIGURE 18 New RADIUS client configuration window



New RADIUS Client

☑ Enable this RADIUS client

Name and Address

Friendly name: ICX7450-24P

Address (IP or DNS): 10.20.64.180

Vendor

Specify RADIUS Standard for most RADIUS clients, or select the RADIUS client vendor from the list.

Vendor name: RADIUS Standard

Shared Secret

To manually type a shared secret, click Manual. To automatically generate a shared secret, click Generate. You must configure the RADIUS client with the same shared secret entered here. Shared secrets are case-sensitive.

● Manual ○ Generate

Shared secret: ●●●●●●

Confirm shared secret: ●●●●●●

Additional Options

□ Access-Request messages must contain the Message-Authenticator attribute

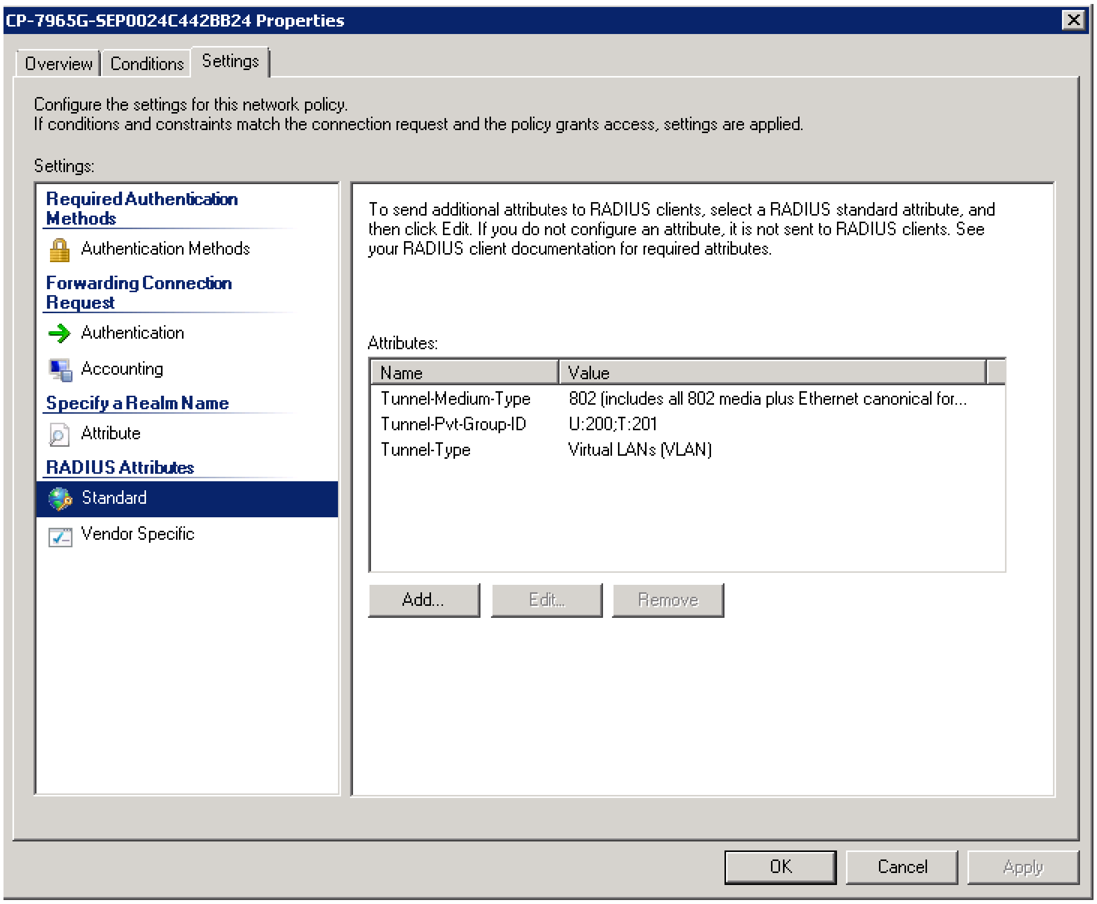
□ RADIUS client is NAP-capable

Step 2: Create a connection request policy for user "CP-7965G-SEP0024C442BB24" and configure following RADIUS attributes. A screen shot of the RADIUS attribute configuration window of network policy server is given in Figure 19 .

TABLE 6 RADIUS attribute for user "CP-7965G-SEP0024C442BB24"

Attribute	Value	Comment
Tunnel-Medium-Type	802	
Tunnel-Pvt-Group-ID	U:200;T:201	The format is U:<data VLAN-id>; T:Voice-VLAN-id> Voice VLAN ID must match the Voice VLAN configuration under interface level where this Phone is connected.
Tunnel-Type	VLAN	

FIGURE 19 RADIUS attribute configuration for user "CP-7965G-SEP0024C442BB24"



CP-7965G-SEP0024C442BB24 Properties

Configure the settings for this network policy.
If conditions and constraints match the connection request and the policy grants access, settings are applied.

Settings:

To send additional attributes to RADIUS clients, select a RADIUS standard attribute, and then click Edit. If you do not configure an attribute, it is not sent to RADIUS clients. See your RADIUS client documentation for required attributes.

Attributes:

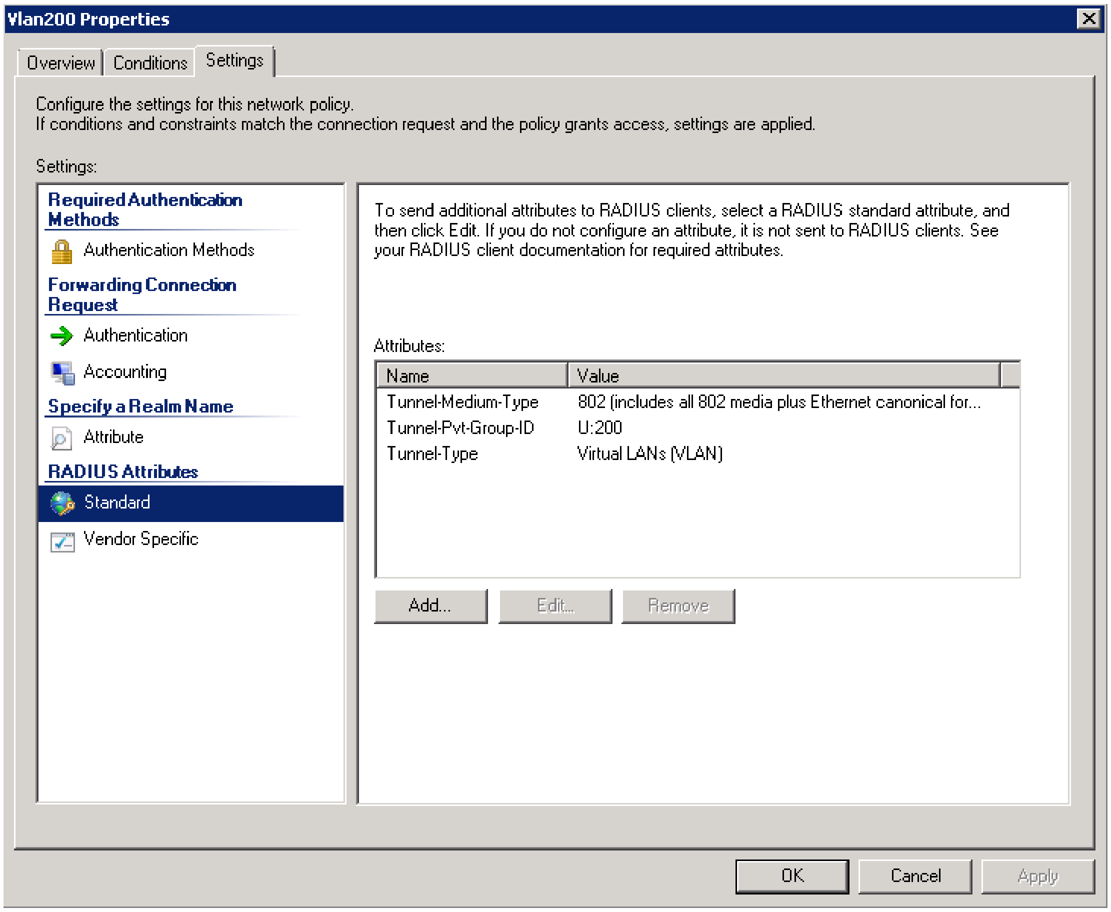
Name	Value
Tunnel-Medium-Type	802 (includes all 802 media plus Ethernet canonical for...
Tunnel-Pvt-Group-ID	U:200;T:201
Tunnel-Type	Virtual LANs (VLAN)

Step 3: Create a connection request policy for user "vlan200" and configure following RADIUS attributes. A screen shot of the RADIUS attribute configuration window of network policy server is given in Figure 20 .

TABLE 7 RADIUS attribute for user "VLAN200"

Attribute	Value	Comment
Tunnel-Medium-Type	802	
Tunnel-Pvt-Group-ID	U:200	The format is U:<VLAN-id> It means untagged traffic from this client will be forwarded in this VLAN
Tunnel-Type	VLAN	

FIGURE 20 RADIUS attribute configuration for user "vlan200"



Configure the settings for this network policy.
If conditions and constraints match the connection request and the policy grants access, settings are applied.

To send additional attributes to RADIUS clients, select a RADIUS standard attribute, and then click Edit. If you do not configure an attribute, it is not sent to RADIUS clients. See your RADIUS client documentation for required attributes.

Name	Value
Tunnel-Medium-Type	802 (includes all 802 media plus Ethernet canonical for...
Tunnel-Pvt-Group-ID	U:200
Tunnel-Type	Virtual LANs (VLAN)

Brocade switch configuration

Step 1: Configure an authentication method list for 802.1X and specify RADIUS as an authentication server. Following CLI configures the 802.1X process on the switch to use the configured RADIUS server to authenticate clients.

```
ICX7450-24P Router(config)#aaa authentication dot1x default radius
```

Step 2: Configure a radius server. In this example, radius server's IP address is 10.20.64.208 and shared key is "secret". The shared key should match the key given during client configuration on

RADIUS server. UDP port 1812 is used for RADIUS authentication messages and UDP port 1813 is used for RADIUS accounting messages.

```
ICX7450-24P Router(config)#radius-server host 10.20.64.208 auth-port 1812 acct-port
1813 default key
secret
```

Step 3: Create a VLAN to be used as auth-default-vlan. This VLAN must be configured to enable authentication. When any port is enabled for dot1x or MAC authentication, the port is moved into this VLAN by default as a MAC-based VLAN member. Sometimes the RADIUS server may authenticate the client but not return the required VLAN information on where the client should be placed. The auth-default VLAN is used in this scenario.

```
ICX7450-24P Router(config)#vlan 5 name auth-default-vlan
ICX7450-24P Router(config-vlan-5)#untagged ethernet 12/1/1
```

Step 4: RADIUS will return VLAN 200 as data VLAN for both phone and PC, this VLAN must exist in the Brocade switch. In this example, virtual interface is also created in this VLAN, so that PC can use the virtual interface IP as its gateway IP.

```
ICX7450-24P Router(config)#vlan 200 name data
ICX7450-24P Router(config-vlan-200)#untagged ethernet 11/1/10 ethernet 12/1/5
ICX7450-24P Router(config-vlan-200)#router-interface ve 200
ICX7450-24P Router(config-vlan-200)#exit
ICX7450-24P Router(config)#int ve 200
ICX7450-24P Router(config-vif-200)#ip address 10.20.74.1/24
ICX7450-24P Router(config-vif-200)#exit
```

Step 5: Create the voice VLAN that will be assigned to the phone by RADIUS. The port that is connected to the phone, must be added to this VLAN as tagged member to be able to configure "voice-vlan" on the port under interface configuration mode. In this example, port 11/1/7 is added to VLAN 201. The virtual interface IP of VLAN 201 will be used as gateway IP for the phone.

```
ICX7450-24P Router(config)#vlan 201 name voice
ICX7450-24P Router(config-vlan-201)#tagged ethernet 11/1/7 to 11/1/8 ethernet 12/1/6
ICX7450-24P Router(config-vlan-201)#router-interface ve 201
ICX7450-24P Router(config-vlan-201)#exit
ICX7450-24P Router(config)#int ve 201
ICX7450-24P Router(config-vif-201)#ip address 172.20.74.1/24
ICX7450-24P Router(config-vif-201)#exit
```

Step 6: Configure IP helper on the virtual interface of the voice VLAN so that DHCP request from the IP phone is forwarded to the call manager. In this topology, call manager's IP address is 10.20.74.31.

```
ICX7450-24P Router(config)#int ve 201
ICX7450-24P Router(config-vif-201)#ip helper-address 1 10.20.74.31
ICX7450-24P Router(config-vif-201)#exit
```

Step 7: Specify which VLAN ID to use as auth-default-vlan under authentication mode. This VLAN must be configured to enable authentication. When any port is enabled for 802.1X or MAC authentication, the port is moved into this VLAN by default as a MAC-based VLAN member. Sometimes the RADIUS server may authenticate the client but not return the required VLAN information on where the client should be placed. The auth-default VLAN is used in this scenario.

```
ICX7450-24P Router(config)#authentication
ICX7450-24P Router(config-authen)#auth-default-vlan 5
```

Step 8: Enable 802.1X on the switch under authentication mode and enable 802.1X on port 11/1/7. Configure port-control mode as "auto" under interface configuration mode. The mode "auto" enables the 802.1X authentication on the interface.

```
ICX7450-24P Router(config)#authentication
ICX7450-24P Router(config-authen)#dot1x enable
ICX7450-24P Router(config-authen)#dot1x enable ethernet 11/1/7
ICX7450-24P Router(config-authen)#exit
ICX7450-24P Router(config)#interface ethernet 11/1/7
ICX7450-24P Router(config-if-e1000-11/1/7)#dot1x port-control auto
ICX7450-24P Router(config-if-e1000-11/1/7)#exit
```

Step 9: Enable PoE on port 11/1/7 using "inline power" CLI and configure voice VLAN 201 under interface configuration mode. The voice-vlan command configures the switch to advertise VLAN 201 as voice VLAN in the CDP messages.

```
ICX7450-24P Router(config)#interface ethernet 11/1/7
ICX7450-24P Router(config-if-e1000-11/1/7)#inline power
ICX7450-24P Router(config-if-e1000-11/1/7)#voice-vlan 201
ICX7450-24P Router(config-if-e1000-11/1/7)#exit
```

Step 10: Enable CDP on the switch. It will enable the switch to respond to Cisco IP phone's CDP messages to negotiate inline power. The switch uses CDP message to communicate voice VLAN information to the IP phone.

```
ICX7450-24P Router(config)#cdp run
```

Step 11: Authentication related configurations are stored under the key word "authentication". To verify authentication related configuration on the switch, use CLI "show running-configuration | begin authentication".

```
ICX7450-24P Router#show running-configuration | begin authentication
authentication
 auth-default-vlan 5
 dot1x enable
 dot1x enable ethe 11/1/7
!
!
!
```

Client authentication and verification

Step 1: Connect phone to port 11/1/7. The phone and switch negotiates inline power using CDP message exchange. The initial power allocation and following adjustment are reported using "PoE" syslogs. After the phone is powered on, ICX7450-24P switch detects the MAC address of phone on port 11/1/7, it prints a syslog indicating that this MAC address is unauthorized and sends "EAP-Request/Identify". After successful RADIUS authentication, the switch sends "EAP-success" message to the client and prints a syslog indicating that the MAC address of Phone is authorized. Refer to Figure 1 on page 5 for more information regarding messages exchanged between client, switch, and RADIUS server.

```
ICX7450-24P Router#

SYSLOG: <14>15d03h50m17s:System: PoE: Allocated power of 95000 mwatts on port
11/1/7.

SYSLOG: <14>15d03h50m22s:System: PoE: Power adjustment done: decreased power by 79600
mwatts on port 11/1/7 .
PoE: Power enabled on port 11/1/7.

SYSLOG: <14>15d03h50m22s:System: PoE: Power enabled on port 11/1/7.

SYSLOG: <14>15d03h50m30s:System: Interface ethernet 11/1/7, state up

SYSLOG: <14>15d03h50m31s:DOT1X: Port 11/1/7 - mac 0024.c442.bb24
AuthControlledPortStatus change:
unauthorized

SYSLOG: <14>15d03h50m31s:DOT1X: Port 11/1/7 - mac 0024.c442.bb24,
AuthControlledPortStatus change:
authorized

SYSLOG: <14>15d03h50m37s:System: PoE: Power adjustment done: decreased power by 3400
mwatts on port 11/1/7
.

ICX7450-24P Router#
ICX7450-24P Router#
```

Step 2: Verification of phone's successful authentication:

- Verify phone is authenticated using "show dot1x sessions ethernet 11/1/7" and look for "PAE (Port Access Entity) state".
- Verify port 11/1/7 is part of VLAN 200 and VLAN 201 using "show vlan 200" and "show vlan 201".
- Verify that the phone received IP from call manager or DHCP server using "show fdp neighbors ethernet 11/1/7".

```
ICX7450-24P Router#show dot1x sessions ethernet 11/1/7
---------------------------------------------------------------------------------------
------

Port        MAC             IP              User         Vlan   Auth       ACL
Age   PAE
            Addr            Addr            Name                State
```

```
State
-------------------------------------------------------------------------------------
-------
11/1/7   0024.c442.bb24  N/A            CP-7965G-SEP002 200  permit  none    Ena
AUTHENTICATED
ICX7450-24P Router#
ICX7450-24P Router#show vlan 200
Total PORT-VLAN entries: 16
Maximum PORT-VLAN entries: 64

Legend: [Stk=Stack-Id, S=Slot]

PORT-VLAN 200, Name data, Priority level0, Spanning tree Off
 Untagged Ports: (U11/M1)  10
 Untagged Ports: (U12/M1)   5
   Tagged Ports: None
   Uplink Ports: None
 DualMode Ports: None
 Mac-Vlan Ports: (U11/M1)   7
     Monitoring: Disabled

ICX7450-24P Router#
ICX7450-24P Router#show vlan 201
Total PORT-VLAN entries: 16
Maximum PORT-VLAN entries: 64

Legend: [Stk=Stack-Id, S=Slot]

PORT-VLAN 201, Name voice, Priority level0, Spanning tree Off
 Untagged Ports: None
   Tagged Ports: (U11/M1)   7   8
   Tagged Ports: (U12/M1)   6
   Uplink Ports: None
 DualMode Ports: None
 Mac-Vlan Ports: None
     Monitoring: Disabled

ICX7450-24P Router#show fdp neighbors ethernet 11/1/7
Device ID: SEP0024C442BB24
Entry address(es):
  IP address: 172.20.74.55
Platform: Cisco IP Phone 7965,  Capabilities: Host
Interface: ethernet11/1/7,  Port ID (outgoing port): Port 1
Holdtime : 141 seconds
SCCP45.9-1-1SR1S
```

Step 3: Ping phone's IP address 172.20.74.55 from the switch to test IP connectivity. As the MAC address of phone is authenticated, ICMP reply from this client will be allowed on port 11/1/7.

```
ICX7450-24P Router#ping 172.20.74.55
Sending 1, 16-byte ICMP Echo to 172.20.74.55, timeout 5000 msec, TTL 64
Type Control-c to abort
Reply from 172.20.74.55    : bytes=16 time<1ms TTL=64
Success rate is 100 percent (1/1), round-trip min/avg/max=0/0/0 ms.
ICX7450-24P Router#
```

Step 4: Connect the PC to phone's PC port. When ICX7450-24P switch detects the MAC address of PC on port 11/1/7, it prints a syslog indicating that this MAC address is unauthorized and sends "EAP-Request/Identify". After successful RADIUS authentication, the switch sends "EAP-success" message to the client and prints a syslog indicating that the MAC address of PC is authorized. Refer to Figure 1 on page 5 for more information regarding messages exchanged between client, switch, and RADIUS server.

```
ICX7450-24P Router#
SYSLOG: <14>15d04h05m14s:DOT1X: Port 11/1/7 - mac 0022.0002.0002
AuthControlledPortStatus change:
unauthorized

SYSLOG: <14>15d04h05m14s:DOT1X: Port 11/1/7 - mac 0022.0002.0002,
AuthControlledPortStatus change:
authorized
```

Step 5: Verify PC is authenticated using "show dot1x sessions ethernet 11/1/7" and look for "PAE(Port Access Entity) State".

```
ICX7450-24P Router#show dot1x sessions ethernet 11/1/7
-------------------------------------------------------------------------------------
-------
```

```
Port        MAC             IP              User         Vlan   Auth       ACL
Age   PAE
            Addr            Addr            Name                State
State
--------------------------------------------------------------------------------------
------
11/1/7   0024.c442.bb24  N/A            CP-7965G-SEP002 200  permit  none    Ena
AUTHENTICATED
11/1/7   0022.0002.0002  N/A            vlan200         200  permit  none    Ena
AUTHENTICATED
ICX7450-24P Router#
```

Step 6: Ping PC's IP address 10.20.74.2 from the switch to test IP connectivity. As the MAC address of PC is authenticated, ICMP reply from this client will be allowed on port 11/1/7.

```
ICX7450-24P Router#ping 10.20.74.2
Sending 1, 16-byte ICMP Echo to 10.20.74.2, timeout 5000 msec, TTL 64
Type Control-c to abort
Reply from 10.20.74.2      : bytes=16 time<1ms TTL=64
Success rate is 100 percent (1/1), round-trip min/avg/max=0/0/0 ms.
ICX7450-24P Router#
```

Deployment consideration

A client may fail to get authenticated in various scenarios This section describes the scenarios and options available to place the client in various VLANs due to authentication failure. This section also provides a brief overview of most used CLIs to troubleshoot common failure events.

- Handling non 802.1X clients using guest VLAN:

  FI 08.0.20 introduces a special VLAN called "guest VLAN". This is applicable when only 802.1X is enabled on a port. MAC authentication is not configured. If guest VLAN is configured, a client MAC is placed in a guest VLAN after 802.1X process times out. Example: Following commands configures VLAN 5 as the guest VLAN. To learn more about guest VLAN, refer to the FastIron 08020 Security Guide.

  ```
  ICX6610-24 Router(config-authen)#dot1x guest-vlan 5
  ```

- Handling 802.1X client without valid credential:

  By default, Brocade switches blocks the MAC address of a client that fails RADIUS authentication. This can happen due expired password or client certificate. Many enterprise customers require failed clients to get limited access to the network so that a new password or certificate can be issued. This can be achieved by moving these MAC to a special VLAN called restricted VLAN. Example: following commands configure VLAN 4 as the restricted VLAN. To learn more about restricted VLAN, refer to the FastIron 08020 Security Guide.

  ```
  ICX6610-24 Router(config)#authentication
  ICX6610-24 Router(config-authen)#restricted-vlan 4
  ICX6610-24 Router(config-authen)#auth-fail-action restricted-vlan
  ```

- Handling temporary RADIUS availability issue

  By default, Brocade switches keeps trying to reach RADIUS server in case of a RADIUS timeout. FI 08.0.20 introduces a special VLAN called "critical VLAN". If this VLAN is configured, client MAC is placed into critical VLAN for a limited time that can be set by "reauth-timeout" (default is 60 seconds) when RADIUS timeout occurs. After "reauth-timeout", Brocade switch tries to authenticate the client again. To learn more about critical VLAN, refer to the FastIron 08020 Security Guide.

  ```
  ICX6610-24 Router(config)#authentication
  ICX6610-24 Router(config-authen)#critical-vlan 3
  ICX6610-24 Router(config-authen)#exit
  ICX6610-24 Router(config)#interface ethernet 1/1/11
  ICX6610-24 Router(config-if-e1000-1/1/11)#authentication timeout-action critical-
  vlan
  ICX6610-24 Router(config-if-e1000-1/1/11)#authentication reauth-timeout 100
  ```

- To deploy MAC authentication, customer need to maintain a MAC database in RADIUS server. To ease deployment in an existing network, Brocade support 3 different MAC address format for RADIUS attribute 1 (username) and RADIUS attribute 2 (password).

```
ICX6610-24 Router(config-authen)#mac-authentication password-format
  xx-xx-xx-xx-xx-xx
  xxxx.xxxx.xxxx
  xxxxxxxxxxxx       (Default)
```

- Brocade supports multiple VLAN assignment on the same port. So each client MAC authenticated via 802.1X or MAC authentication can be assigned to different VLAN. Brocade supports both VLAN number and VLAN name in RADIUS attribute 81 (Tunnel-private-group-ID). For example:

  Tunnel-private-group-ID = U:100, or

  Tunnel-private-group-ID = U:Marketing
- In windows operating systems, DHCP is a parallel event, independent of 802.1X authentication which starts once interface comes up. If 802.1X authentication take too long, DHCP may time out; if this issue is encountered in a network, Brocade recommends configuring MAC authentication as the authentication method.
- Common flexible authentication authorization failure:
  - Brocade device in not configured as client on the RADIUS server
  - Invalid RADIUS attribute sent via RADIUS access-accept. Please refer to the appropriate use case for required attributes and syntax in each scenario.

Troubleshooting

Brocade recommends using following commands to understand which issue is causing an authentication failure:

- Using syslog feature
- "debug dot1x event:

A truncated output of "debug dot1x event" is given below for a scenario when the VLAN ID provided in access-accept message from RADIUS does not match any existing VLAN on the switch.

```
22d 22:47:01: 802.1X: port 2/1/11:[220002,2] Tx EAPOL PDU with packet type EAP
-Packet containing EAP Request packet to RADIUS Server at RESPONSE state of Backend
Auth SM with EAP Id: 2

22d 22:47:01: 802.1X: backend state for port 2/1/11:[220002,2] is RESPONSE

22d 22:47:01: 802.1X: Rx AAA_ACCEPT for port 2/1/11:0022.0002.0002 from
authentication server

22d 22:47:01: 802.1X: port 2/1/11:[220002,2] is passed the info of Tunnel-Type=13;
Tunnel_Medium_Type=6; Tunnel_Private_Group_ID=U:51

22d 22:47:01: 802.1X: vlan_name (String): 51 is now converted to vlan id (Decimal):
51
RADIUS assigned vlan 51 does not exist

22d 22:47:01: 802.1X: port 2/1/11: [220002:2]  Unable to assign VLAN as mandated by
RADIUS - failed
the client

22d 22:47:01: 802.1X: port 2/1/11:[220002,2] Tx EAPOL Pkt at FAIL State of Backend
Auth SM with EAP
Code: 0x04 (Failure), EAP Id: 2

22d 22:47:01: 802.1X: authenticator state for port 2/1/11:[220002,2] is HELD
dot1x add session sent

22d 22:47:01: 802.1X: backend state for port 2/1/11:[220002,2] is FAIL

22d 22:47:01: 802.1X: backend state for port 2/1/11:[220002,2] is IDLE

SYSLOG: <14>Oct 16 14:46:27 DOT1X: Port 2/1/11 - mac 0022.0002.0002
AuthControlledPortStatus change: unauthorized
```

Upgrade consideration

The following behavior associated with flexible authentication should be taken into consideration when upgrading to FastIron 08.0.20 or later.

802.1x authentication and MAC authentication configured on default VLAN

After upgrading to FastIron 08.0.20 or later, global configuration for both 802.1X authentication and MAC authentication move under the authentication command, and the first unused VLAN becomes auth-default-vlan (the authentication default VLAN), VLAN 2 in the following example. Interface level configuration for 802.1X authentication and MAC authentication conform to any new CLI changes that are part of the upgrade.

For example, before upgrade, with 802.1X authentication enabled on port 2/1/24 and MAC authentication enabled on 2/1/23 globally and at the interface level, the configured ports are part of the default VLAN. After upgrade, since port 2/1/23 and 2/1/24 are part of the default VLAN, they become part of the auth-default-vlan, VLAN 2 in this example.

```
vlan 1 name DEFAULT-VLAN by port >> 2/1/24 and 2/1/23 ports are part of default vlan
!
vlan 3 by port
tagged ethe 1/1/5
!
vlan 100 by port
tagged ethe 1/1/9
untagged ethe 1/1/18
!
vlan 200 by port
untagged ethe 1/1/15
!
vlan 201 by port
!
dot1x-enable >> global configuration
enable ethe 2/1/24
!
mac-authentication enable >> global configuration
mac-authentication auth-passwd-format xxxx.xxxx.xxxx
!
interface ethernet 2/1/24 >> interface level
dot1x port-control auto
!
interface ethernet 2/1/23 >> interface level
mac-authentication enable
mac-authentication enable-dynamic-vlan
mac-authentication max-accepted-session 32
```

The following example shows the configuration after the upgrade.

```
vlan 1 name DEFAULT-VLAN by port
!
vlan 2 by port
!
vlan 3 by port
tagged ethe 1/1/5
!
vlan 100 by port
tagged ethe 1/1/9
untagged ethe 1/1/18
!
vlan 200 by port
untagged ethe 1/1/15
!
vlan 201 by port
!
authentication >>> both dot1x and mac-auth global commands appears under
authentication command
auth-default-vlan 2
```

```
dot1x enable
dot1x enable ethe 2/1/24
mac-authentication enable
mac-authentication enable ethe 2/1/23
mac-authentication password-format xxxx.xxxx.xxxx
!
interface ethernet 2/1/23
authentication max-sessions 32
!
interface ethernet 2/1/24
dot1x port-control auto
```

802.1X authentication and MAC authentication configured on a VLAN other than the default VLAN

After upgrading to FastIron 08.0.20 or later, global configuration for both 802.1X authentication and MAC authentication move under the authentication command, and the first unused VLAN becomes auth-default-vlan, VLAN 2 in the following example.

For example, before upgrade, with 802.1X authentication enabled globally on port 2/1/24 and MAC authentication enabled globally on port 2/1/23, the configured ports are part of VLANs 600 and 601. After upgrade, VLAN 600 becomes the auth-default-vlan for port 2/1/24, and 601 becomes the auth-default-vlan for port 2/1/23.

```
vlan 1 name DEFAULT-VLAN by port
!
vlan 3 by port
tagged ethe 1/1/5
!
vlan 100 by port
tagged ethe 1/1/9
untagged ethe 1/1/18
!
vlan 200 by port
untagged ethe 1/1/15
!
vlan 201 by port
!
vlan 600 by port
untagged ethe 2/1/24 or tagged ethe 2/1/24
!
vlan 601 by port
untagged ethe 2/1/23 or tagged ethe 2/1/23
!
dot1x-enable >> global configuration
enable ethe 2/1/24
!
mac-authentication enable >> global configuration
mac-authentication auth-passwd-format xxxx.xxxx.xxxx
!
interface ethernet 2/1/24 >> interface level
dot1x port-control auto
!
interface ethernet 2/1/23 >> interface level
mac-authentication enable
mac-authentication enable-dynamic-vlan
mac-authentication max-accepted-session 32
```

The following example shows the configuration after the upgrade.

```
vlan 1 name DEFAULT-VLAN by port
!
vlan 2 by port
!
vlan 3 by port
tagged ethe 1/1/5
!
vlan 100 by port
tagged ethe 1/1/9
untagged ethe 1/1/18
!
vlan 200 by port
```

```
untagged ethe 1/1/15
!
vlan 201 by port
!
vlan 600 by port >> 2/1/24 should be removed
!
vlan 601 by port >> 2/1/23 should be removed
!
authentication
auth-default-vlan 2
dot1x enable
dot1x enable ethe 2/1/24
mac-authentication enable
mac-authentication enable ethe 2/1/23
mac-authentication password-format xxxx.xxxx.xxxx
!
interface ethernet 2/1/24
authentication auth-default-vlan 600
dot1x port-control auto
!
interface ethernet 2/1/23
authentication auth-default-vlan 601
authentication max-sessions 32
!
```

802.1X authentication and MAC authentication configured on a voice VLAN

After upgrading to FastIron 08.0.20 or later, global configuration for both 802.1X authentication and MAC authentication moves under the authentication command. The first unused VLAN moves as auth-default-vlan (the authentication default VLAN), VLAN 2 in the following example. Any dual-mode commands on the interface are replaced by the auth-default-vlan at the interface level. The voice-vlan command remains the same.

For example, before upgrade, with dot1x authentication enabled globally on port 2/1/24 and MAC authentication enabled globally on port 2/1/23, the configured ports are part of VLANs 100 and 200 respectively as tagged. Both of these ports are also part of voice-vlan VLAN 1000 as tagged. After the upgrade, VLAN 100 becomes auth-default-vlan for port 2/1/24, and VLAN 200 becomes auth-default-vlan for port 2/1/23. The voice-vlan 1000 command is retained.

```
vlan 1 name DEFAULT-VLAN by port
!
vlan 3 by port
tagged ethe 1/1/5
!
vlan 100 by port
tagged ethe 1/1/9 ethe 2/1/24
untagged ethe 1/1/18
!
vlan 200 by port
tagged ethe 2/1/23
untagged ethe 1/1/15
!
vlan 1000 by port
tagged ethe 2/1/23 to 2/1/24
!
dot1x-enable >> global configuration
enable ethe 2/1/24
!
mac-authentication enable >> global configuration
mac-authentication auth-passwd-format xxxx.xxxx.xxxx
!
interface ethernet 2/1/24 >> interface level
dot1x port-control auto
dual-mode 100
voice-vlan 1000
!
interface ethernet 2/1/23 >> interface level
mac-authentication enable
mac-authentication enable-dynamic-vlan
mac-authentication max-accepted-session 32
```

```
dual-mode 200
voice-vlan 1000
```

The following example shows the configuration after the upgrade.

```
FCX_Stack(2U)# sh run vlan
vlan 1 name DEFAULT-VLAN by port
!
vlan 2 by port
!
vlan 3 by port
tagged ethe 1/1/5
!
vlan 100 by port
tagged ethe 1/1/9 >> 2/1/24 should be removed
untagged ethe 1/1/18
!
vlan 200 by port >> 2/1/23 should be removed
untagged ethe 1/1/15
!
vlan 1000 by port
tagged ethe 2/1/23 to 2/1/24
!
authentication
auth-default-vlan 2
dot1x enable
dot1x enable ethe 2/1/24
mac-authentication enable
mac-authentication enable ethe 2/1/23
mac-authentication password-format xxxx.xxxx.xxxx
!
interface ethernet 2/1/24
authentication auth-default-vlan 100
dot1x port-control auto
voice-vlan 1000
!
interface ethernet 2/1/23
authentication auth-default-vlan 200
authentication max-sessions 32
voice-vlan 1000
!
```