53-1004158-01
18 December 2015

Brocade FastIron Flexible Authentication

Deployment Guide

Supporting FastIron 08.0.40

BROCADE

Contents

Preface

Introduction

Brocade ICX switches running FastIron software support Network Access Control features, including IEEE 802.1X, MAC authentication, and Web authentication. These authentication methods can be used to address various use cases in granting network access to users and devices.

FastIron release 8.0.20 introduced the Flexible Authentication feature, or Flex Auth, which provides the flexibility to use authentication methods such as 802.1X and MAC authentication. Both mechanisms can be used in a configurable sequence for additional flexibility, depending on the use case of authenticating a user or a device or a combination of both. This flexibility also helps to reduce authentication traffic, and it provides a common configuration set that can be used across all ports on a switch regardless of the clients connecting to it.

Flexible Authentication allows the network administrator to set the sequence of authentication methods to be attempted on a switch port. This feature supports two methods: 802.1X authentication 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 retain feature parity when they upgrade their switches from versions prior to 8.0.20.

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

Purpose of This Document

The purpose of this deployment guide is to provide an understanding of Flex Auth and the steps required to successfully configure and deploy a strong set of authentication schemes suitable for your network. This guide describes the following use cases:

1. Dynamic VLAN and ACL Assignment with MAC Authentication
2. Dynamic VLAN and ACL Assignment with 802.1X Authentication
3. Dynamic VLAN and ACL Assignment with Default Authentication Order
4. Dynamic VLAN and ACL Assignment with Authentication Order—MAC Authentication Followed by 802.1X
5. Authentication of a Phone and a PC on the Same Port Using Flexible Authentication

Audience

This document can be used by many, including technical marketing engineers, system engineers, technical assistance center engineers, and customers to deploy a Flexible Authentication scheme for a network.

Related Documents

In addition to this deployment guide, see the following guides, which focus on a particular NAC application server, such as Cisco ISE and Aruba ClearPass.

- *Brocade FastIron Flexible Authentication Deployment Guide with Aruba ClearPass*
- *Brocade FastIron Flexible Authentication Deployment Guide with Cisco ISE*
- *FastIron Ethernet Switch Security Configuration Guide* (08.0.20)
- *Brocade FastIron Security Configuration Guide* (08.0.40)
- *IEEE 802.1X-2004*

  http://www.ieee802.org/1/pages/802.1x-2004.html
- *PPP 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	Part Number	Description
December 2015	53-1004158-01	Initial release.

Overview

802.1X Authentication

The 802.1X-based authentication is a standards-based implementation, and it defines three types of device roles in a network:

- Client/Supplicant
- Authenticator
- Authentication Server

Client/Supplicant—The devices (for example, desktop, laptop, IP phone) that seek to gain access to the network. Clients must be running software that supports the 802.1X standard. Clients can be directly connected to a port on the authenticator, or they can be connected via 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.

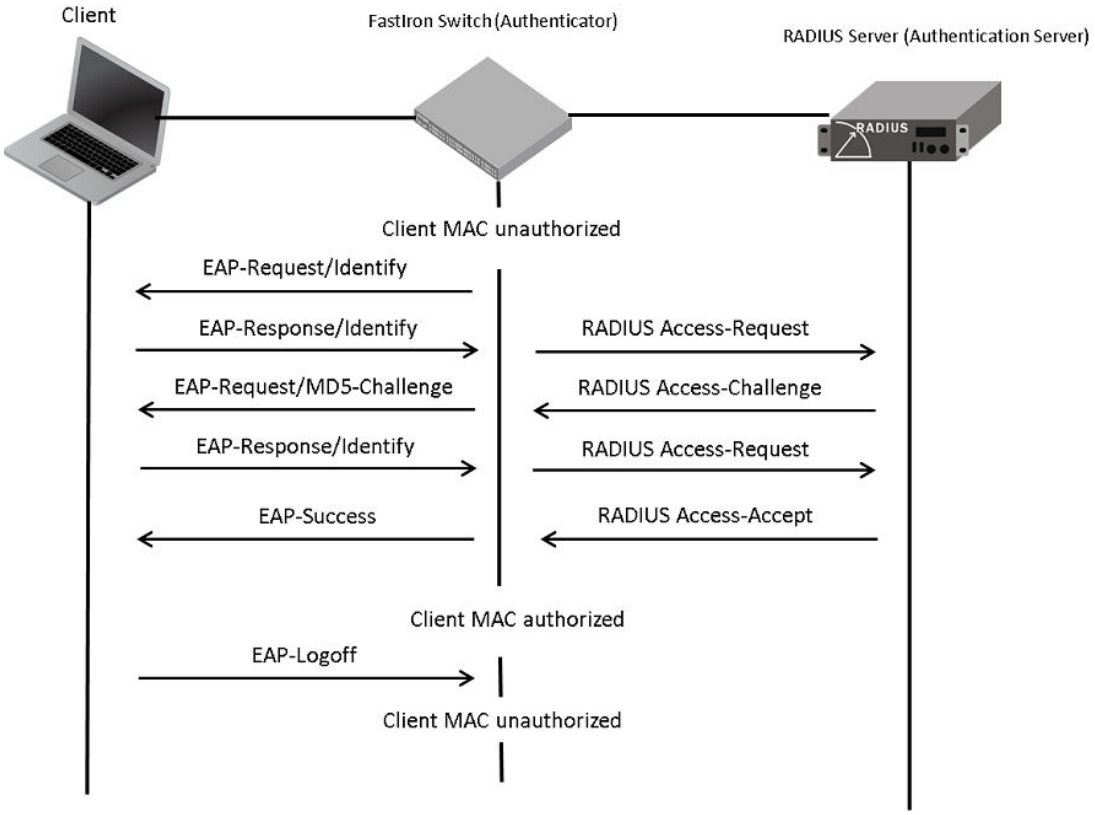
Authentication Server—The device that validates the client and specifies whether the client may access services on the device. Brocade supports authentication servers that run RADIUS.

Message Exchange During Authentication

For communication between 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 the 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 a password. The authenticator passes this information to the authentication server, which determines whether the client can access services provided by the authenticator. If authentication succeeds, the MAC address of the client is authorized. In addition, the RADIUS server may include a network access policy, such as a dynamic VLAN or an 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 be 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 to 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. In this situation, the administrator can decide to grant some or the same access as original instead of blocking the access. This VLAN should be configured with the desired access levels.

Restricted VLAN—When 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 the 802.1X feature, refer to the *Brocade FastIron Security Configuration 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 a RADIUS server successfully authenticates the source MAC address. The MAC address itself is used as the username and password for RADIUS authentication; the user does not provide a specific username and password to gain access to the network. If RADIUS authentication for that MAC address succeeds, traffic from that MAC address is forwarded.

If the RADIUS server cannot validate the user's MAC address, 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 via the CLI. The MAC authentication feature supports the use of a critical VLAN and a restricted VLAN, as described in the “802.1X Authentication” section.

For more information about the MAC authentication feature, refer to the *Brocade FastIron Security Configuration Guide*.

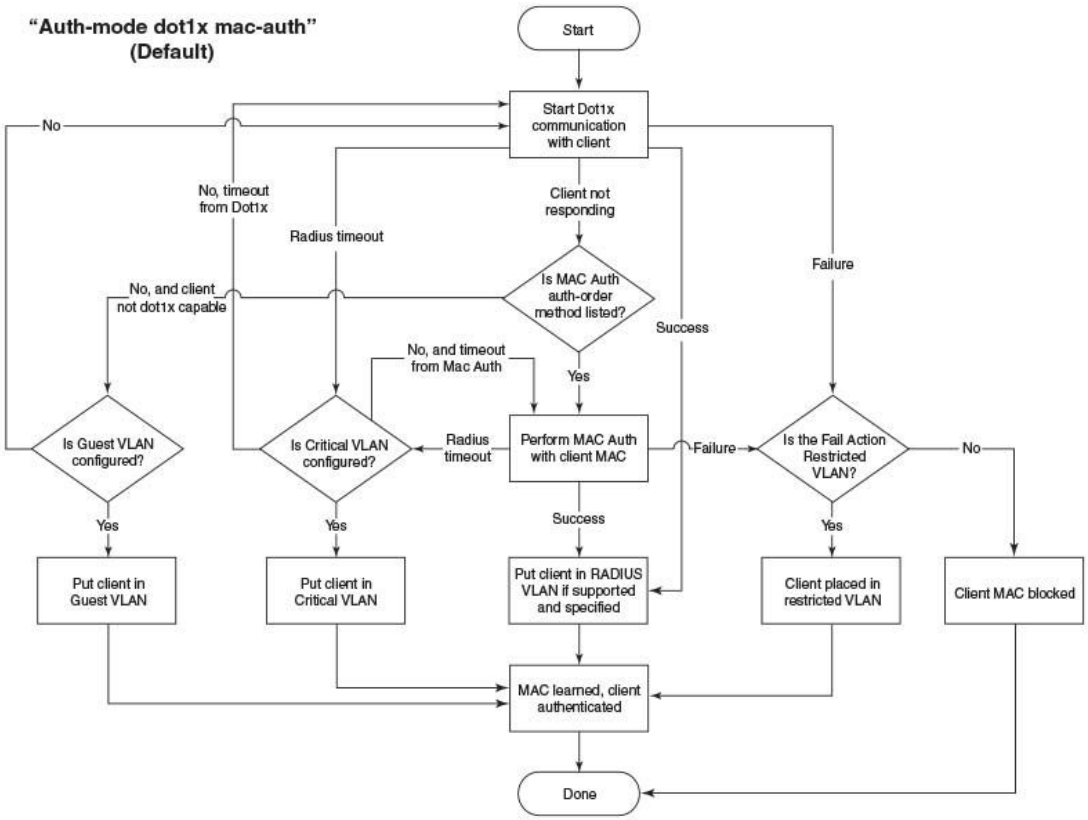
Flexible Authentication

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 authentication and MAC authentication. By default the sequence is set to 802.1X.

How Flexible Authentication Works

The following flow chart explains how flexible authentication is implemented in FastIron. 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.

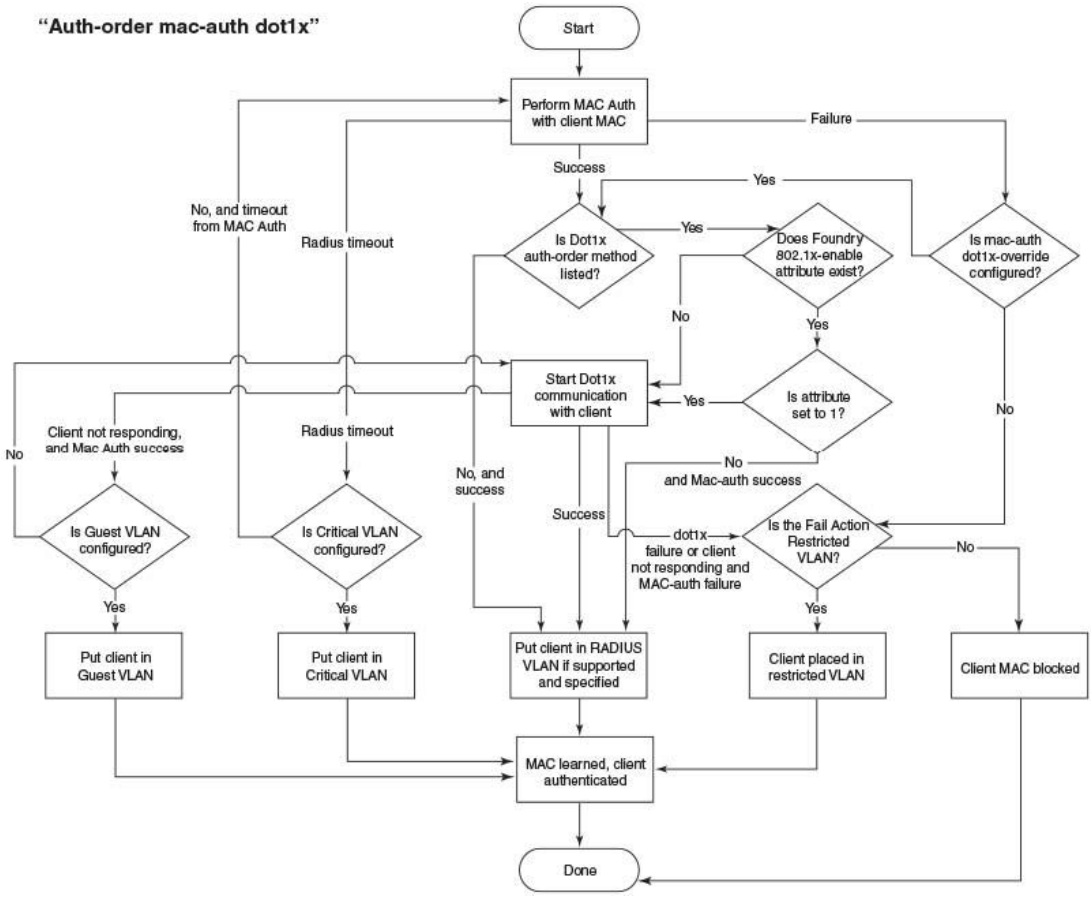
FIGURE 2 Default Sequence—802.1X Followed by MAC Authentication



When the sequence is set to MAC authentication followed 802.1X:

- MAC authentication is attempted first. If it succeeds, the 802.1X method is also attempted.
- If MAC authentication succeeds, the 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 the 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 fails, 802.1X is not attempted and the configured failure action is taken. However, the administrator can configure the **dot1x-override** command through the CLI to allow the clients that failed MAC authentication to authenticate via the 802.1X method.

FIGURE 3 MAC Authentication Followed by 802.1X



Platform Support for Flexible Authentication

Flexible Authentication was designed to work on all campus switching products. Flexible Authentication support was introduced in release 08.0.20. The following platforms are supported:

- FCX
- ICX 6430
- ICX 6450
- ICX 6610
- ICX 7250
- ICX 7450
- ICX 7750

FastIron 08.0.40 supports only the following platforms:

- ICX 7250
- ICX 7450
- ICX 7750

NOTE
From FastIron 08.0.30d and later, by default, FCX, ICX 6430, ICX 6450, ICX 6610, and ICX 7000 platforms support two clients per port. Support for a higher number of clients per port can be configured using the CLI.

Dynamic VLAN and ACL Assignment with MAC Authentication

The following example uses MAC authentication for authenticating a client and then dynamically assigns a VLAN and ACL after a successful authentication.

Client A

- The MAC address is 0010.9400.8402.
- After authentication:
  - The client should be placed in VLAN 3.
  - Incoming traffic from client A should be filtered by ACL 102.

FreeRADIUS Configuration

```
001094008402   Cleartext-Password := "001094008402"
Filter-ID = ip.102.in,
Tunnel-Type = 13,
Tunnel-Medium-Type = 6,
Tunnel-Private-Group-ID = U:3
```

Switch Configuration

```
!
vlan 2 name global-auth-default-vlan by port
!
vlan 3 by port
 untagged ethe 2/1/2
!
authentication
 auth-default-vlan 2
 mac-authentication enable
 mac-authentication enable ethe 2/1/1
!
aaa authentication dot1x default radius
radius-server host 10.20.64.11 auth-port 1812 acct-port 1813 default key secret
!
access-list 102 deny ip any 10.11.0.0 0.255.255.255
access-list 102 permit ip any any
!
```

Switch Output

```
SYSLOG: <13> Sep 28 19:06:38 ICX-Switch MAC Authentication succeeded for [0000.1094.8402 ] on port
2/1/1
ICX-Switch# show mac-authentication sessions all
--------------------------------------------------------------------------------
Port        MAC              IP              Vlan  Auth      ACL     Age
            Addr             Addr                  State
--------------------------------------------------------------------------------
2/1/1       0000.1094.8402   192.168.1.2     3     Yes       in-102  Ena

ICX-Switch# show vlan 3
Total PORT-VLAN entries: 16
Maximum PORT-VLAN entries: 4095

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

PORT-VLAN 3, Name [None], Priority level0, Spanning tree On
```

```
 Untagged Ports: (U2/M1)   2
   Tagged Ports: None
   Uplink Ports: None
 DualMode Ports: None
 Mac-Vlan Ports: (U2/M1)   1
     Monitoring: Disabled

ICX-Switch# show mac-auth ip-acl e 2/1/1
MAC-Auth IP ACL Information :

Port 2/1/1 : 0000.1094.8402
In-bound IP ACL : 102
ICX-Switch#
```

Dynamic VLAN and ACL Assignment with 802.1X Authentication

The following example uses 802.1X authentication for authenticating a client and then dynamically assigns a VLAN and ACL after a successful authentication.

Client A

- Username: user8402
- Password: password
- After authentication:
  - The client should be placed in VLAN 3.
  - Incoming traffic from client A should be filtered by ACL 102.

FreeRADIUS Configuration

```
user8402 Cleartext-Password := "password"
Tunnel-Type = 13,
Tunnel-Medium-Type = 6,
Tunnel-Private-Group-ID = U:3,
Filter-ID = ip.102.in
```

Switch Configuration

```
!
vlan 2 name global-auth-default-vlan by port
!
vlan 3 by port
 untagged ethe 2/1/2
!
authentication
 auth-default-vlan 2
 dot1x enable
 dot1x enable ethe 2/1/1
!
interface ethernet 2/1/1
 dot1x port-control auto
!
aaa authentication dot1x default radius
radius-server host 10.20.64.11 auth-port 1812 acct-port 1813 default key secret
!
access-list 102 deny ip any 10.11.0.0 0.255.255.255
access-list 102 permit ip any any
!
```

Switch Output

```
SYSLOG: <14> Sep 28 19:12:50 ICX-Switch DOT1X: Port 2/1/1 - mac 0000.1094.8402,
AuthControlledPortStatus change: authorized

ICX-Switch# show dot1x sessions all
-------------------------------------------------------------------------------------------------------
Port        MAC              IP             User          Vlan  Auth      ACL     Age   PAE
            Addr             Addr           Name                State                   State
-------------------------------------------------------------------------------------------------------
```

```
2/1/1       0000.1094.8402    192.168.1.2     user8402      3     permit    in-102  Ena   AUTHENTICATED


ICX-Switch# show vlan 3
Total PORT-VLAN entries: 16
Maximum PORT-VLAN entries: 4095

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

PORT-VLAN 3, Name [None], Priority level0, Spanning tree On
 Untagged Ports: (U2/M1)   2
   Tagged Ports: None
   Uplink Ports: None
 DualMode Ports: None
 Mac-Vlan Ports: (U2/M1)   1
     Monitoring: Disabled

ICX-Switch# show dot1x ip-acl e 2/1/1
802.1X IP ACL Information :

Port 2/1/1 : 0000.1094.8402
In-bound IP ACL : 102
ICX-Switch#
```

Dynamic VLAN and ACL Assignment with Default Authentication Order

This use case demonstrates how Flexible Authentication works with the client undergoing 802.1X authentication and MAC authentication. The default sequence of authentication is 802.1x first followed by MAC authentication.

Client A

- Client MAC address: 0010.9400.8402
- 802.1x username: user8402
- Password: password
- After authentication:
  - The client should be placed in VLAN 3.
  - Incoming traffic from client A should be filtered by ACL 102.

FreeRADIUS Configuration

```
user8402 Cleartext-Password := "password"
Tunnel-Type = 13,
Tunnel-Medium-Type = 6,
Tunnel-Private-Group-ID = U:3,
Filter-ID = ip.102.in

001094008402   Cleartext-Password := "001094008402"
Filter-ID = ip.102.in,
Tunnel-Type = 13,
Tunnel-Medium-Type = 6,
Tunnel-Private-Group-ID = U:3
```

Switch Configuration

```
!
vlan 2 name global-auth-default-vlan by port
!
vlan 3 by port
 untagged ethe 2/1/2
!
authentication
 auth-default-vlan 2
 dot1x enable
 dot1x enable ethe 2/1/1
 mac-authentication enable
 mac-authentication enable ethe 2/1/1
!
interface ethernet 2/1/1
 dot1x port-control auto
!
aaa authentication dot1x default radius
radius-server host 10.20.64.11 auth-port 1812 acct-port 1813 default key secret
!
access-list 102 deny ip any 10.11.0.0 0.255.255.255
access-list 102 permit ip any any
!
```

Switch Output (Successful Case)

```
SYSLOG: <14> Sep 28 19:36:32 ICX-Switch DOT1X: Port 2/1/1 - mac 0000.1094.8402,
AuthControlledPortStatus change: authorized

ICX-Switch# show dot1x sessions all
-------------------------------------------------------------------------------------------------------
Port        MAC              IP              User          Vlan  Auth      ACL     Age   PAE
            Addr             Addr            Name                State                   State
-------------------------------------------------------------------------------------------------------
2/1/1       0000.1094.8402   192.168.1.2     user8402      3     permit    in-102  Ena   AUTHENTICATED

ICX-Switch# show mac-auth se all
-----------------------------------------------------------------------
Port        MAC              IP              Vlan  Auth      ACL     Age
            Addr             Addr                  State
-----------------------------------------------------------------------
ICX-Switch#

ICX-Switch# show vlan 3
Total PORT-VLAN entries: 16
Maximum PORT-VLAN entries: 4095

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

PORT-VLAN 3, Name [None], Priority level0, Spanning tree On
 Untagged Ports: (U2/M1)   2
   Tagged Ports: None
   Uplink Ports: None
 DualMode Ports: None
 Mac-Vlan Ports: (U2/M1)   1
     Monitoring: Disabled

ICX-Switch# show dot1x ip-acl e 2/1/1
802.1X IP ACL Information :

Port 2/1/1 : 0000.1094.8402
In-bound IP ACL : 102
ICX-Switch#
```

Switch Output (Client Is Not dot1x Capable)

```
SYSLOG: <14> Nov  3 21:09:41 ICX-Switch DOT1X: Port 2/1/1 - mac 0010.9400.8402 AuthControlledPortStatus
change: unauthorized

SYSLOG: <13> Nov  3 21:10:00 ICX-Switch MAC Authentication succeeded for [0010.9400.8402 ] on port
2/1/1

ICX-Switch# show dot1x se all
-------------------------------------------------------------------------------------------------------
Port        MAC              IP              User          Vlan  Auth      ACL     Age   PAE
            Addr             Addr            Name                State                   State
-------------------------------------------------------------------------------------------------------
2/1/1       0010.9400.8402   N/A             N/A           3     init      none    Ena   HELD
ICX-Switch#
ICX-Switch# show mac-auth se all
-----------------------------------------------------------------------
Port        MAC              IP              Vlan  Auth      ACL     Age
            Addr             Addr                  State
-----------------------------------------------------------------------
2/1/1       0010.9400.8402   192.168.1.2     3     Yes       in-102  Ena

ICX-Switch# show vlan 3
Total PORT-VLAN entries: 20
Maximum PORT-VLAN entries: 4095

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

PORT-VLAN 3, Name isolation, Priority level0, Spanning tree Off
 Untagged Ports: (U2/M1)   2
   Tagged Ports: None
   Uplink Ports: None
 DualMode Ports: None
```

```
 Mac-Vlan Ports: (U2/M1)   1
     Monitoring: Disabled

ICX-Switch# show dot1x ip-acl e 2/1/1
802.1X IP ACL Information :

Port 2/1/1 : 0010.9400.8402
ICX-Switch#

ICX-Switch# show mac-auth ip-acl e 2/1/1
MAC-Auth IP ACL Information :

Port 2/1/1 : 0010.9400.8402
In-bound IP ACL : 102
ICX-Switch#
```

Dynamic VLAN and ACL Assignment with Authentication Order —MAC Authentication Followed by 802.1X

This use case demonstrates how Flexible Authentication works with the client undergoing MAC authentication and 802.1X authentication. The sequence of authentication is MAC authentication followed by 802.1X. This is a nondefault sequence and must be manually configured using the **auth-order mac-auth dot1x** command. This sequence is typically used when upgrading from an earlier version of software (FastIron 8.0.10 or earlier). When this sequence is used, both MAC authentication and 802.1x authentication for that client must pass. If a RADIUS authentication process is successful, the RADIUS server sends an Access-Accept message to the switch, authenticating the client. The Access-Accept message can include vendor-specific attributes (VSAs) that specify additional information about the device. Brocade VSAs can be used to make this sequence more flexible. The Brocade Vendor-ID is 1991 with Vendor-Type 1.

1. If the client is only 802.1X capable, you can use the **mac-authentication dot1x-override** command under the port to try 802.1X after a MAC authentication failure.
2. If the client is not 802.1X capable, you can skip 802.1X authentication after a successful MAC authentication by using a VSA on the RADIUS server: attribute name, Foundry-802_1x-enable; attribute ID, 6. If the value is set to 0, the switch does not attempt 802.1X authentication. If the value is set to 1 or if the attribute is not present, the switch attempts 802.1X authentication.
3. If the client is not 802.1X capable, you can use the client MAC address for 802.1X authentication by specifying both the username and password as the MAC address and also by using a VSA on the RADIUS server: attribute name, Foundry-802_1x-valid; attribute ID, 7. If the value is set to 0, a user is prevented from using the MAC address as the username and password for 802.1X authentication. If the value is set to 1, the RADIUS record is valid for both MAC authentication and 802.1X authentication. A user can use the MAC address as username and password for 802.1X authentication.

If the client fails MAC authentication in this particular Flex Auth sequence, the client is blocked and no traffic from the client is forwarded by the switch.

Client A

- The client MAC address: 0010.9400.8402
- 802.1x username: user8402
- Password: password
- After authentication:
  - The client should be placed in VLAN 3.
  - Incoming traffic from client A should be filtered by ACL 102.

FreeRADIUS Configuration

```
user8402 Cleartext-Password := "password"
Tunnel-Type = 13,
Tunnel-Medium-Type = 6,
Tunnel-Private-Group-ID = U:3,
Filter-ID = ip.102.in

001094008402   Cleartext-Password := "001094008402"
Filter-ID = ip.102.in,
Tunnel-Type = 13,
Tunnel-Medium-Type = 6,
Tunnel-Private-Group-ID = U:3
```

Switch Configuration

```
!
vlan 2 name global-auth-default-vlan by port
!
vlan 3 by port
 untagged ethe 2/1/2
!
authentication
 auth-order mac-auth dot1x
 auth-default-vlan 2
 dot1x enable
 dot1x enable ethe 2/1/1
 mac-authentication enable
 mac-authentication enable ethe 2/1/1
!
interface ethernet 2/1/1
 dot1x port-control auto
!
aaa authentication dot1x default radius
radius-server host 10.20.64.11 auth-port 1812 acct-port 1813 default key secret
!
access-list 102 deny ip any 10.11.0.0 0.255.255.255
access-list 102 permit ip any any
!
```

Switch Output (Successful Case)

```
SYSLOG: <13> Sep 28 20:39:29 ICX-Switch MAC Authentication succeeded for [0000.1094.8402 ] on port
2/1/1
SYSLOG: <14> Sep 28 20:39:29 ICX-Switch DOT1X: Port 2/1/1 - mac 0000.1094.8402,
AuthControlledPortStatus change: authorized
ICX-Switch# show mac-auth ip-acl e 2/1/1
MAC-Auth IP ACL Information :
ICX-Switch# show mac-auth se all
--------------------------------------------------------------------------------
Port        MAC               IP              Vlan  Auth      ACL     Age
            Addr              Addr                  State
--------------------------------------------------------------------------------
2/1/1       0000.1094.8402    192.168.1.2     3     Yes       none    Ena

ICX-Switch# show dot1x session all
--------------------------------------------------------------------------------------------------------------
Port        MAC               IP              User          Vlan  Auth      ACL     Age   PAE
            Addr              Addr            Name                State                   State
--------------------------------------------------------------------------------------------------------------
2/1/1       0000.1094.8402    192.168.1.2     user8402      3     permit    in-102  Ena   AUTHENTICATED

ICX-Switch# show vlan 3
Total PORT-VLAN entries: 16
Maximum PORT-VLAN entries: 4095

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

PORT-VLAN 3, Name [None], Priority level0, Spanning tree On
 Untagged Ports: (U2/M1)   2
   Tagged Ports: None
   Uplink Ports: None
 DualMode Ports: None
 Mac-Vlan Ports: (U2/M1)   1
     Monitoring: Disabled
ICX-Switch#
ICX-Switch# show mac-auth ip-acl e 2/1/1
MAC-Auth IP ACL Information :
ICX-Switch# show dot1x ip-acl e 2/1/1
802.1X IP ACL Information :

Port 2/1/1 : 0000.1094.8402
In-bound IP ACL : 102
ICX-Switch#
```

Switch Output (MAC Authentication Failure Case)

```
SYSLOG: <13> Sep 30 00:15:12 ICX-Switch DOT1X: Port 2/1/1 Mac 0000.1094.8402 - MAC authentication
failed for MAC 0000.1094.8402 as RADIUS server rejected
SYSLOG: <9> Sep 30 00:15:12 ICX-Switch MAC Authentication failed for [0000.1094.8402 ] on port 2/1/1
(Invalid User)
ICX-Switch# show mac-auth se all
-----------------------------------------------------------------------
Port        MAC             IP              Vlan  Auth      ACL     Age
            Addr            Addr                  State
-----------------------------------------------------------------------
2/1/1       0000.1094.8402  N/A             4092  No        none    H45
ICX-Switch# show dot1x se all
-------------------------------------------------------------------------------------------------------
Port        MAC             IP              User          Vlan  Auth      ACL     Age   PAE
            Addr            Addr            Name                State                   State
-------------------------------------------------------------------------------------------------------
ICX-Switch#
ICX-Switch# show vlan 3
Total PORT-VLAN entries: 15
Maximum PORT-VLAN entries: 4095

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

PORT-VLAN 3, Name [None], Priority level0, Spanning tree On
 Untagged Ports: (U2/M1)   2
   Tagged Ports: None
   Uplink Ports: None
 DualMode Ports: None
 Mac-Vlan Ports: None
     Monitoring: Disabled
ICX-Switch#
```

Switch Output (MAC Authentication Failure Case with dot1x Override)

```
authentication
 auth-order mac-auth dot1x
 auth-default-vlan 2
 dot1x enable
 dot1x enable ethe 2/1/1
 mac-authentication enable
 mac-authentication enable ethe 2/1/1
 mac-authentication dot1x-override

SYSLOG: <9> Sep 30 00:20:24 ICX-Switch MAC Authentication failed for [0000.1094.8402 ] on port 2/1/1
(Invalid User)
SYSLOG: <14> Sep 30 00:20:24 ICX-Switch DOT1X: Port 2/1/1 - mac 0000.1094.8402,
AuthControlledPortStatus change: authorized

ICX-Switch# show mac-auth se all
-----------------------------------------------------------------------
Port        MAC             IP              Vlan  Auth      ACL     Age
            Addr            Addr                  State
-----------------------------------------------------------------------
2/1/1       0000.1094.8402  N/A             3     No        none    H40
ICX-Switch# show dot1x se all
-------------------------------------------------------------------------------------------------------
Port        MAC             IP              User          Vlan  Auth      ACL     Age   PAE
            Addr            Addr            Name                State                   State
-------------------------------------------------------------------------------------------------------
2/1/1       0000.1094.8402  192.168.1.2     user8402      3     permit    in-102  Ena   AUTHENTICATED
ICX-Switch#

ICX-Switch# show vlan 3
Total PORT-VLAN entries: 15
Maximum PORT-VLAN entries: 4095

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

PORT-VLAN 3, Name [None], Priority level0, Spanning tree On
 Untagged Ports: (U2/M1)   2
   Tagged Ports: None
   Uplink Ports: None
```

```
 DualMode Ports: None
 Mac-Vlan Ports: (U2/M1)   1
     Monitoring: Disabled
ICX-Switch#
ICX-Switch# show dot1x ip-acl e 2/1/1
802.1X IP ACL Information :

Port 2/1/1 : 0000.1094.8402
In-bound IP ACL : 102
ICX-Switch#
```

Authentication of a Phone and a PC on the Same Port Using Flexible Authentication

This use case demonstrates the use for Flexible Authentication in a setup where a PC is daisy-chained to an IP phone connected to a switch port. When Flexible Authentication is enabled on a port with an IP phone and a PC, both clients go through 802.1X and MAC authentication. It is typical to use MAC authentication for the IP phone and 802.1X for the PC connecting to the phone. The following example shows the configuration and validation of this use case.

Note that if the IP phone is not capable of participating in the 802.1X process, it will time out and then MAC authentication is tried. If the IP phone is capable of 802.1X, 802.1X authentication is used first by default. If it succeeds, MAC authentication is not performed.

In FastIron 8.0.40, the LLDP configuration for the IP phone can also be automated using the RADIUS attributes. In the following example, we have defined the voice VLAN, DSCP, and Priority values in the RADIUS server.

- Tunnel-Private-Group-ID = T:48,
- Foundry-Voice-Phone-Config = "dscp:46;priority:4"

If LLDP is not configured via the RADIUS server, the following LLDP configuration must be added to enable LLDP MED on the port connecting to the IP phone.

```
lldp med network-policy application voice tagged vlan 48 priority 4 dscp 46 ports
ethernet 2/1/1
```

Client A

- The client MAC address: 0cd9.9690.1ed3
- 802.1x username: user8402
- Password: password
- After authentication:
  - The client should be placed in VLAN 3 and the IP phone in tagged VLAN 48.
  - Incoming traffic from client A should be filtered by ACL 102.

FreeRADIUS Configuration

```
user8402 Cleartext-Password := "password"
Tunnel-Type = 13,
Tunnel-Medium-Type = 6,
Tunnel-Private-Group-ID = U:3,
Filter-ID = ip.102.in

0cd996901ed3 Cleartext-Password := "0cd996901ed3"
Tunnel-Type = 13,
Tunnel-Medium-Type = 6,
Tunnel-Private-Group-ID = T:48,
Foundry-Voice-Phone-Config = "dscp:46;priority:4"
```

Switch Configuration

```
!
vlan 2 name global-auth-default-vlan by port
!
vlan 3 by port
```

```
 untagged ethe 2/1/2
!
authentication
 auth-default-vlan 2
 dot1x enable
 dot1x enable ethe 2/1/1
 mac-authentication enable
 mac-authentication enable ethe 2/1/1
!
interface ethernet 2/1/1
 dot1x port-control auto
 inline power
!
aaa authentication dot1x default radius
radius-server host 10.20.64.11 auth-port 1812 acct-port 1813 default key secret
!
access-list 102 deny ip any 10.11.0.0 0.255.255.255
access-list 102 permit ip any any
!
lldp run
!
```

Switch Output

```
SYSLOG: <14> Nov  5 20:03:57 ICX-Switch DOT1X: Port 2/1/1 - mac 0010.9400.8402,
AuthControlledPortStatus change: authorized

SYSLOG: <13> Nov  5 20:04:11 ICX-Switch MAC Authentication succeeded for [0cd9.9690.1ed3 ] on port
2/1/1

SYSLOG: <13> Nov  5 20:04:14 ICX-Switch MAC Authentication succeeded for [0cd9.9690.1ed3 ] on port
2/1/1

ICX-Switch# show dot1x se all
--------------------------------------------------------------------------------------------------------
Port        MAC               IP              User          Vlan  Auth      ACL     Age   PAE
            Addr              Addr            Name                State                   State
--------------------------------------------------------------------------------------------------------
2/1/1       0010.9400.8402    192.168.1.2     user8402      3     permit    in-102  Ena   AUTHENTICATED
2/1/1       0cd9.9690.1ed3    N/A             N/A           3     init      none    Ena   HELD
ICX-Switch#

ICX-Switch# show mac-auth se all
-----------------------------------------------------------------------------
Port        MAC               IP              Vlan  Auth      ACL     Age
            Addr              Addr                  State
-----------------------------------------------------------------------------
2/1/1       0cd9.9690.1ed3    N/A             48    Yes       none    Ena
2/1/1       0cd9.9690.1ed3    N/A             3     Yes       none    Ena
ICX-Switch#

ICX-Switch# show vlan 3
Total PORT-VLAN entries: 22
Maximum PORT-VLAN entries: 4095

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

PORT-VLAN 3, Name isolation, Priority level0, Spanning tree Off
 Untagged Ports: None
   Tagged Ports: (U2/M1)   2
   Uplink Ports: None
 DualMode Ports: None
 Mac-Vlan Ports: (U2/M1)   1
     Monitoring: Disabled
ICX-Switch#

ICX-Switch# show vlan 48
Total PORT-VLAN entries: 22
Maximum PORT-VLAN entries: 4095

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

PORT-VLAN 48, Name [None], Priority level0, Spanning tree On
 Untagged Ports: None
```

```
   Tagged Ports: (U2/M1)   1   2
   Uplink Ports: None
 DualMode Ports: None
 Mac-Vlan Ports: None
     Monitoring: Disabled
ICX-Switch#

ICX-Switch# show lldp local-info port e 2/1/1
Local port: 2/1/1
  + Chassis ID (MAC address): cc4e.24b4.2222
  + Port ID (MAC address): cc4e.24b4.7bc0
  + Time to live: 120 seconds
  + System name         : "ICX-Switch"
  + Port description    : "GigabitEthernet2/1/1"
  + System description  : "Brocade Communications Systems, Inc. Stacking Syste\
                           m ICX7250-24-HPOE, IronWare Version 08.0.40q072T213\
                            Compiled on Nov  3 2015 at 21:33:12 labeled as SPR\
                           08040q072"
  + System capabilities : bridge, router
    Enabled capabilities: bridge, router
  + 802.3 MAC/PHY          : auto-negotiation enabled
    Advertised capabilities: 10BaseT-HD, 10BaseT-FD, 100BaseTX-HD,
                             100BaseTX-FD, fdxSPause, fdxBPause, 1000BaseT-HD,
                             1000BaseT-FD
    Operational MAU type   : 1000BaseT-FD
  + Link aggregation: not capable
  + Maximum frame size: 10200 octets
  + MED capabilities: capabilities, networkPolicy, location, extendedPSE
    MED device type : Network Connectivity
  + MED Network Policy
    Application Type  : Voice
    Policy Flags      : Known Policy, Tagged
    VLAN ID           : 48
    L2 Priority       : 4
    DSCP Value        : 46
  + Port VLAN ID: none
  + Management address (IPv4): 10.20.64.39

ICX-Switch# show dot1x ip-acl e 2/1/1
802.1X IP ACL Information :

Port 2/1/1 : 0010.9400.8402
In-bound IP ACL : 102

Port 2/1/1 : 0cd9.9690.1ed3
ICX-Switch#
```