Cisco IOS Quick Reference Guide for IBNS

Cisco® IBNS is the foundation for providing access control to corporate networks. The Cisco IBNS solution is a set of Cisco IOS® Software services designed to enable secure user and host access to enterprise networks powered by Cisco Catalyst® switches and WLANs. This Quick Reference Guide allows technical personnel to quickly bring up IBNS with sample configurations for Monitor Mode, Low Impact Mode, and High Security Mode as well as for other commonly used tasks.

For more information about Cisco IBNS, please visit http://www.cisco.com/go/IBNS.

Global Switch Identity Settings (Applicable to All IBNS Modes)	
Cisco IOS AAA Settings	
`switch(config)# aaa new-model`	Enables authentication, authorization, and accounting (AAA)
`switch(config)# aaa authentication dot1x default group radius`	Creates an 802.1X port-based authentication method list
`switch(config)# aaa authorization network default group radius`	Required for VLAN/access control list (ACL) assignment
`switch(config)# aaa accounting dot1x default start-stop group radius`	Enables 802.1X accounting and MAC Address Bypassing (MAB)
Cisco IOS RADIUS	
`switch(config)# radius-server host aaa.server.ip* auth-port 1645 acct-port 1646` * The ip address for your AAA server (for example, Cisco Access Control Server [ACS] 5.0).	Specifies the IP address of the RADIUS server
`switch(config)# radius-server key user-defined-shared-key (e.g.,pa$$wor6)**` `** You may wish to use a different shared key. Just make sure it is the same as the one you entered into ACS when defining the AAA client.`	Specifies the preshared key
Cisco IOS 802.1X	
`switch(config)# dot1x system-auth-control`	Globally enables 802.1X port-based authentication
ACS 5.0	
Refer to the section Getting Started with Global Configuration Settings in the IBNS Phased Deployment Guide.	

Basic Identity Switch Port Configuration (Basic Switch Port Configuration)	
Identity settings to be added to the access ports	
Example: Interface range g2/1-16	Example range to apply the port configuration to
`switch(config-if)# authentication port-control auto`	Enables port-based authentication on the interface
`switch(config-if)# dot1x pae authenticator`	Enables 802.1X authentication on the interface
`switch(config-if)# mab`	Enables MAB
`switch(config-if)# end`	

Cisco Catalyst Identity Feature Support

NOTE: This quick reference guide primarily focuses on the newer features supported across the Catalyst portfolio as shown in the table here. This is not an exhaustive list of all supported features. Consult the product and Cisco IOS Software documentation for a complete list of supported features and command references.

NOTE: The Cisco IOS Software releases listed here are considered the baseline[1] for new Identity Based Networking Services features. Please consider using these releases or later versions for deploying of IBNS.

	Identity Features	Catalyst 6500 12.2(33)SXI2	Catalyst 4500 12.2(50)SG	Catalyst 2K3K 12.2(50)SE
Authentication	IEEE 802.1x authentication	Y	Y	Y
	MAC Authentication Bypass	Y	Y	Y
	Local Web Authentication	Y	Y	Y
	Flexible authentication	Y	Y	Y
	Multi-host	Y	Y	Y
	Multi-domain Auth (MDA)	Y	Y	Y
	Multi-host	Y	Y	Y
Policy Enforcement	VLAN assignment	Y	Y	Y
	VVLAN with CDP Bypass	Y	Y	Y
	Guest VLAN, Auth-Fail VLAN, PVLAN	Y	Y	Y
	Downloadable ACL	Y	Y	Y
Infrastructure integration	Open Access (Monitor & Low Impact Modes)	Y	Y	Y
	Wake-on-LAN (WoL)	Y	Y	Y
	Radius supplied time out	Y	Y	Y
	Critical port (aka IAB)	Y	Y	Y
	Inactivity aging (MAB and 802.1x)	Y	Y	Y
	CDP enhancement for second port disconnect	Y	Y	Y
	Integration with DAI, IPSG, port security	Y	Y	Y
Instrumentation	MIB	Y	Y	Y
	Radius accounting	Y	Y	Y
	Conditional logging/debugging	Y	Y	Y

IBNS Deployment Modes

(Optional) Monitor Mode (Switch Port Configuration)

Identity settings to be added to the basic IBNS access ports

Example: Interface range g2/1-16 `switch(config-if)# authentication open`	Example range to apply the port configuration to **Enables preauthentication open access (nonrestricted)**
`switch(config-if)# authentication host-mode multi-auth`	Allows a single IP phone and one or more data clients to authenticate independently on an authorized port. Each host, or MAC address, is authenticated individually.

[1] IBNS IOS Software baseline versions: Catalyst 6500, 12.2(33)SXI2; Catalyst 4500, 12.2(50)SG; or Catalyst 3xxx/2xxx , 12.2(50)SE or later.

(Optional) Low Impact Mode (Global Configurations)	
Identity settings to be added to the access ports	**Note**: You must configure a downloadable ACL (dACL) on ACS, as well as an authorization profile to apply and therefore download the ACL, prior to enabling this mode on the switch. For more information on dACLs and ACS refer to the Low Impact Mode section in the IBNS Phased Deployment Guide .
Global switch configuration additions for Low Impact Mode	
`switch(config)# radius-server vsa send authentication` `switch(config)# ip device tracking`	In order to enable dACLs, you must first configure your access switch to allow communications using the cisco-av-pair attribute with the value aaa:event=acl-download. Enter the command shown here in the global configuration of the switch. Failure to add this command will result in failed authentication/authorization requests. Configures the IP device tracking table, which is also required to use dACLs. The downloadable ACL feature allows you to download device-specific authorization policies from the authentication server. These policies activate after authentication succeeds for the respective client and the client's IP address has been populated in the IP device tracking table. (The downloadable ACL is applied on the port once the port is authenticated and the IP device tracking table has the host IP address entry.)
Preauthentication Ingress Port ACL (Example) – Prerequsuite Basic and Monior Mode Settings	

`switch(config)#ip access-list extended PRE-AUTH`
`switch(config)# remark Allow DHCP`
`switch(config)# permit udp any eq bootpc any eq bootps`
`switch(config)# remark Allow DNS`
`switch(config)# permit udp any any eq domain`
`switch(config)#  remark Deny all else`
`switch(config)# deny ip any any`
	IP- based ACL to be applied to selected ports
	The use of ingress ACLs is also a requirement in order to allow successful authorizations that include downloadable ACLs. Failure to add ingress ACLs will result in failed authentication/authorizations.

Low Impact Mode (Switch Port Configurations)	
Switch interface configuration additions/changes for Low Impact Mode	

Example: Interface range g2/1-16
`switch(config-if)#ip access-group PRE-AUTH in`
`switch(config-if)#authentication host-mode multi-domain`
	Applies the previously configured static extended ACL to the desired/applicable ports.
	Sets the authorization manager mode on the Low Impact Mode ports to "multi-domain".

Low Impact Mode (Specific Show Commands)	
Show commands to help verify application of dCALs	

`switch# show ip device tracking all`
`switch# show epm session ip x.x.x.x`
 	
`switch# show ip access-list`
`switch# show ip access-list interface <int-id>`
	Displays the IP device tracking table that contains the host IP addresses learned through Address Resolution Protocol (ARP) or Dynamic Host Configuration Protocol (DHCP).
	Using the IP address learned from the IP device tracking table **show** command above, specify the IP address as the required option for the **show epm session ip** command to verify whether the dACL was successfully downloaded from ACS.
	Displays the extended IP access lists configured on the switch
	Displays the extended IP access list applied to the specified interface

High Security Mode (Switch Port Configurations)	
The primary difference for High Security Mode over Monitor and Low Impact Modes is the requirement to successfully authenticate prior to any traffic (other than Estensible Authentication Protocol over LAN [EAPoL]) allowed on the network. This is considered traditional closed mode behavior of IEEE 802.1X.	

`Example: Interface range g2/1-16`
`switch(config-if)#no authentication open`
`switch(config-if)#no ip access-group PRE-AUTH in`
	High Security Mode does not use the authentication open feature.
	The premise of having an ingress ACL is to restrict traffic flows based on the content of the ACL. Since no traffic can flow through the port, this feature is not a requirement. However, High Security Mode does not preclude the use of ingress ACLs. In fact, if you want to use dACLs for your authorization, an ingress ACL is required. Traditionally, the authorization method for High Security Mode is dynamic VLAN assignment. This is not mandatory, but is an option as well.

Additional IBNS Port Configuration Commands (Switch Port Configurations)

Authentication Related

Host-Mode Settings

```
Example: Interface range g2/1-16
switch(config-if)#authentication host-mode
[multi-auth | multi-domain | multi-host | single-host]
or
switch(config-if)#dot1x host-mode {single-host |
multi-host | multi-domain
```

Note: the default host mode is single, unless otherwise configured through the authentication host-mode command. The port will be in one of the host modes if 802.1X is enabled. Below are the different modes to chose from.

- **multi-auth**: Allows one client on the voice VLAN and multiple authenticated clients on the data VLAN

  Note: The multi-auth keyword is only available with the authentication host-mode command.
- **multi-host**: Allows multiple hosts on an 802.1x-authorized port after a single host has been authenticated
- **multi-domain**: Allows both a host and a voice device, such as an IP phone (Cisco or non Cisco), to be authenticated on an 802.1x-authorized port

  Note: You must configure the voice VLAN for the IP phone when the host mode is set to multidomain.
- **single-host**: Allows a single host (client) on an 802.1x-authorized port

Make sure that the authentication port control or dot1x port-control interface configuration command set is set to auto for the specified interface.

Host Mode Summary

Host Mode	Enforcement	Deployment Considerations
Single	Single mac address per port	• Second mac address triggers a security violation • VMs on the host must share the same mac address. • CDP Bypass is the only IPT solution.
Multi-Domain Auth (MDA)	One Voice Device + One Data Device per port	• Same as single host mode except phone authenticates • Supports third party phones
Multi-Auth	Superset of MDA with multiple Data Devices per port	• Authenticates every mac address in the data domain. • VMs on the host may use different mac addresses. • One VLAN (default port VLAN) for all devices on the port
Multi-Host	One authenticated device allows any number of subsequent mac addresses.	• Not recommended • VMs on the host may use different mac addresses. • CDP Bypass is the only IPT solution.

FlexAuth

Flexible Authentication (FlexAuth)[2] is a set of features that allows IT administrators to enable multiple authentication methods on a single port and to configure the sequence and priority of 802.1X, MAB, and switch-based web authentication (local WebAuth).

Use the reference above in the authentication section for the commands to enable 802.1X, MAB, or WebAuth. By default, the authentication order and priority is 802.1X then MAB and then WebAuth. Use the commands below to modify the default behavior.

`switch(config-if)# authentication order [dot1x | mab] | {webauth}`	(Optional) Sets the order of authentication methods used on a port
`switch(config-if)# authentication priority [dot1x | mab] | {webauth}`	(Optional) Sets the priority of the authentication methods

Please refer to the Deployment Note document that covers FlexAuth, Order, and Priority considerations. *[FLEX-AUTH ORDERING & PRIORITY APP NOTE]*

Local WebAuth

See the WebAuth section for full configuration.

802.1X with unidirectional controlled port (WoL)

```
switch(config-if)# authentication control-direction
{in | both}
or
Pre-BASELINE IBNS support
switch(config-if)# dot1x control-direction {in | both}
```

(Optional) Enables unidirectional port control on each port

When you configure a port as **bidirectional** with the **authentication control-direction both** interface configuration command (or the **dot1x control-direction both interface** configuration command for Pre-BASELINE IBNS Cisco IOS Software releases), the port is access controlled in both directions. In this state, except for EAPoL packets, a switch port does not receive or send packets.

[2] FlexAuth is available across the Catalyst portfolio starting with the IBNS Cisco IOS Software baseline: Catalyst 6500, 12.2(33)SXI2; Catalyst 4500, 12.2(50)SG; or Catalyst 3xxx/2xxx, 12.2(50)SE or later.

Additional Optional IBNS Port Configuration Commands (Switch Port Configurations)	
Authentication Related (Continued)	
Security violation disposition	
`switch(config-if)# authentication violation [shutdown | restrict]`	(Optional) Configures the disposition of the port if a security violation occurs. The default action is to shut down the port. If the **restrict** keyword is configured, the port does not shut down, but trap entries are installed for the violating MAC address, and traffic from that MAC address is dropped. Useful command for IP telephony and multihost/multiuser deployments
Periodic reauthentication	

`switch(config-if)# authentication periodic`
 	
`or`
 	
`Pre-BASELINE IBNS support`
`switch(config-if)# dot1x reauthentication`
	(Optional) Enables periodic reauthentication of the client, which is disabled by default

`Switch(config-if)# authentication timer {{[inactivity | reauthenticate] [server | am]} {restart value}}`
 	
`or`
 	
`Pre-BASELINE IBNS support`
`switch(config-if)# dot1x timeout reauth-period {seconds | server}`
	(Optional) Sets the number of seconds between reauthentication attempts
	The authentication timer keywords have these meanings:
	• **inactivity**: Interval in seconds of inactivity, after which client activity is considered unauthorized
	• **reauthenticate**: Time in seconds after which an automatic reauthentication attempt is to be initiated
	• **server am**: Interval in seconds after which an attempt is made to authenticate an unauthorized port
	• **restart value**: Interval in seconds after which an attempt is made to authenticate an unauthorized port
	The dot1x timeout reauth-period keywords have these meanings:
	• **seconds**: Sets the number of seconds from 1 to 65535; the default is 3600 seconds.
	• **server**: Sets the number of seconds based on the value of the Session-Timeout RADIUS attribute (Attribute[27]) and the Termination-Action RADIUS attribute (Attribute [29]).
	This command affects the behavior of the switch only if periodic reauthentication is enabled.

`switch(config-if)# dot1x timeout quiet-period seconds`	(Optional) When the switch cannot authenticate the client, the switch remains idle for a set period of time and then tries again. The **dot1x timeout quiet-period** interface configuration command controls the idle period. A failed client authentication might occur because the client provided an invalid password. You can provide a faster response time to the user by entering a number smaller than the default. Sets the number of seconds that the switch remains in the quiet state after a failed authentication exchange with the client. The range is 1 to 65535 seconds; the default is 60.
`Switch(config-if)# dot1x timeout tx-period seconds`	(Optional) The client responds to the EAP request/identity frame from the switch with an EAP response/identity frame. If the switch does not receive this response, it waits a set period of time (known as the retransmission time) and then resends the frame. Sets the number of seconds that the switch waits for a response to an EAP request/identity frame from the client before resending the request. The range is 1 to 65535 seconds; the default is 5. **Note**: You should change the default value of this command only to adjust for unusual circumstances such as unreliable links or specific behavioral problems with certain clients and authentication servers.
`Switch(config-if)# dot1x max-req count`	(Optional) You can change the number of times that the switch sends an EAP request/identity frame (assuming no response is received) to the client before restarting the authentication process. Sets the number of times that the switch sends an EAP request/identity frame to the client before restarting the authentication process. The range is 1 to 10; the default is 2. Note: You should change the default value of this command only to adjust for unusual circumstances such as unreliable links or specific behavioral problems with certain clients and authentication servers.

Additional Optional IBNS Port Configuration Commands (Switch Port Configurations)	
Authentication Related (Continued)	
Switch(config-if)# **dot1x max-reauth-req** count	(Optional) You can also change the number of times that the switch restarts the authentication process before the port changes to the unauthorized state. Sets the number of times that the switch restarts the authentication process before the port changes to the unauthorized state. The range is 0 to 10; the default is 2.
Switch(config-if)# **dot1x max-req** count	(Optional) Used to set the number of times that the switch sends an EAP request/identity frame to the client before restarting the authentication process. The range is 1 to 10; the default is 2. Note: This feature is rarely used. It controls how many times the switch will retransmit an EAP packet if no response is received from a previously communicative supplicant.
Switch(config)# **authentication timer reauthenticate server**	(Optional) **RADIUS-provided session timeouts** The 802.1x RADIUS-supplied timeout feature allows a switch to determine the duration of a session and the action to take when the session's timer expires.
Manually re-authenticating 802.1X clients	
switch# **dot1x re-authenticate interface** interface-id	(Optional) Use this command to manually re-authenticate the client connected to a specific port at any time. Note you can just initiate **dot1x re-authenticate** to re-authenticate all 802.1X-enabled ports on the switch.
(Optional) Authorization – Locally Administered	
Guest VLAN	
New BASELINE IBNS Features[3] switch(config-if)# **authentication event no-response action authorize vlan** vlan-id or Pre-BASELINE IBNS support switch(config-if)# **dot1x guest-vlan** vlan-id	(Optional) Specifies an active VLAN as an 802.1x guest VLAN. The range is 1 to 4094. You can configure any active VLAN except an internal VLAN (routed port), an RSPAN VLAN, a primary private VLAN, or a voice VLAN as an 802.1x guest VLAN.
Auth-Fail	
New BASELINE IBNS Features switch(config-if)#**authentication event fail action authorize** vlan-id or Pre-BASELINE IBNS support switch(config-if)# **dot1x auth-fail vlan** vlan-id	(Optional) Specifies an active VLAN as an 802.1x restricted VLAN. The range is 1 to 4094. You can configure any active VLAN except an internal VLAN (routed port), an RSPAN VLAN, a primary private VLAN, or a voice VLAN as an 802.1x restricted VLAN. When you configure a restricted VLAN on a switch, clients that are 802.1x compliant are moved into the restricted VLAN when the authentication server does not receive valid credentials. The switch supports restricted VLANs only in single-host mode.
switch(config-if)# **dot1x auth-fail max-attempts** number	(Optional) You can configure the maximum number of authentication attempts allowed before a user is assigned to the restricted VLAN by using the **dot1x auth-fail max-attempts** interface configuration command. The range of allowable authentication attempts is 1 to 3. The default is 3 attempts.
switch(config-if)# **authentication event fail action next-method**	(Optional) Specifies that the next configured authentication method be applied if authentication fails. **Note**: You should make sure that you have a secondary authentication method configured before enabling this command.

[3] Next-Generation Cisco IOS Software features supported on Catalyst 6500 running 12.2(33)SXI2, Catalyst 4500 running Cisco IOS Software 12.2(50)SG, and Catalyst 3K/2K running Cisco IOS Software 12.2(50)SE or later versions.

(Optional) Authorization – Locally Administered (continued)	
Critical Auth (aka Inaccessible Authentication Bypass)	
New BASELINE IBNS Features switch(config-if)# **authentication event server dead action authorize vlan** or Pre-BASELINE IBNS support switch(config-if)# **dot1x critical vlan** vlan-id	(Optional) Enables the Critical Auth (aka, Inaccessible Authentication Bypass) feature on the port To disable the feature, use the **no authentication event server dead action authorize vlan** interface configuration command (for earlier releases, use the **no dot1x critical** interface configuration command).
New BASELINE IBNS Features switch(config-if)# **authentication event server alive action reinitialize** or Pre-BASELINE IBNS support switch(config-if)# **dot1x critical recovery action reinitialize**	(Optional) Specifies that the port should be reinitialized if it is critically authorized and RADIUS becomes available The default is not to reinitialize the port.

(Optional) Authorization – Centrally Administered

dACLs (Downloadable ACLs)

Switch Configuration

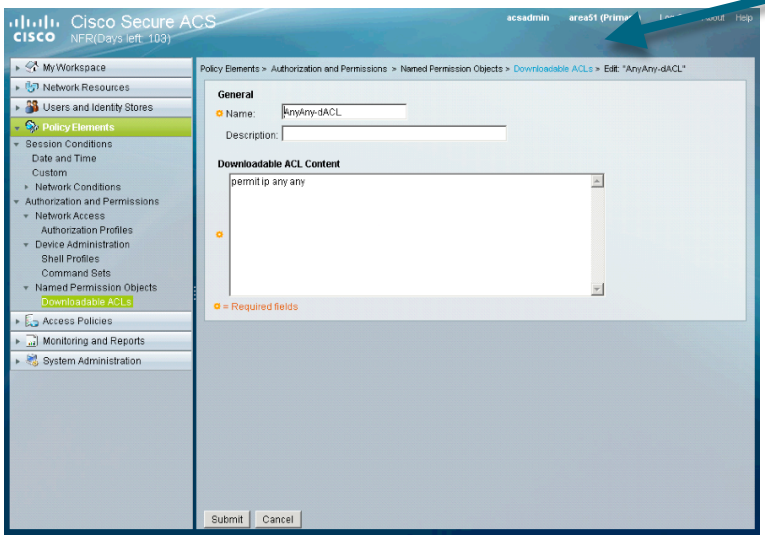
```
switch(config-if)# ip access-group ACL-NAME* in
```

** where ACL-NAME is the name of the ACL you defined in your global config. See the Monitor-mode section above for an example PACL named PRE-AUTH.*

In order to allow RADIUS based authorization of dACLs, the access port is currently required to have a Ingress Port Based ACL (PACL) applied to the port, otherwise the authorization will fail.

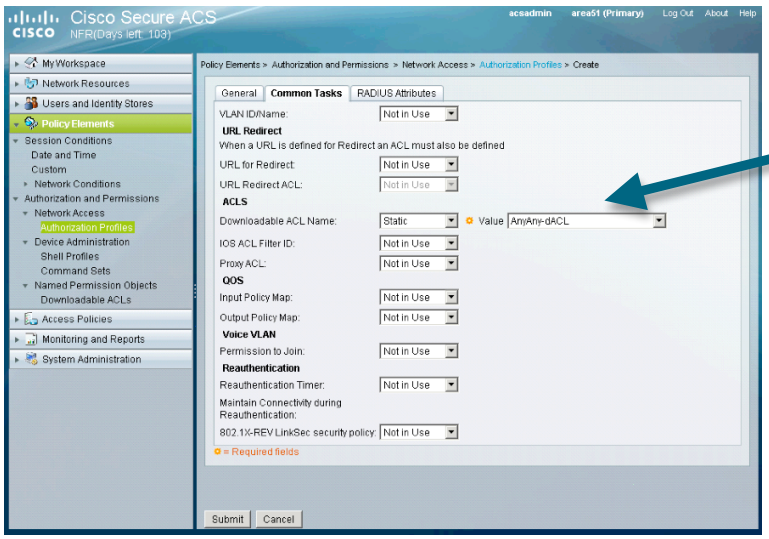
ACS 5.1 Configuration Example

Create a Named Downloadable ACL (dACL) – Example



Navigate to Downloadable ACLs which is found under Policy Elemnets -> Authorizations and Permssions -> Named Permission Objects. From here you can add, edit or delete dACLs. These dACLs will be used later in the Authorization Profiles. In this example we have created a dACL named AnyAny-dACL.

Apply the Named dACL to an authorization profile



Here we have applied the named dACL (AnyAny-dACL) to this particular named Authorization Profile which has been named CorpUser. This Authorization Profile is now available for use with any of the define Access Services (e.g., 802.1X, MAB or WebAuth).

For more information on ACS 5.x configuration refer to Scenario Based Identity Based Networking Services Deployments
http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6586/ps6638/whitepaper_C11-530469.html

(Optional) Authorization – Centrally Administered (continued)

ACLs (RADIUS Filter-ID Attribute)

Switch Configuration

Example numbered ip ACL

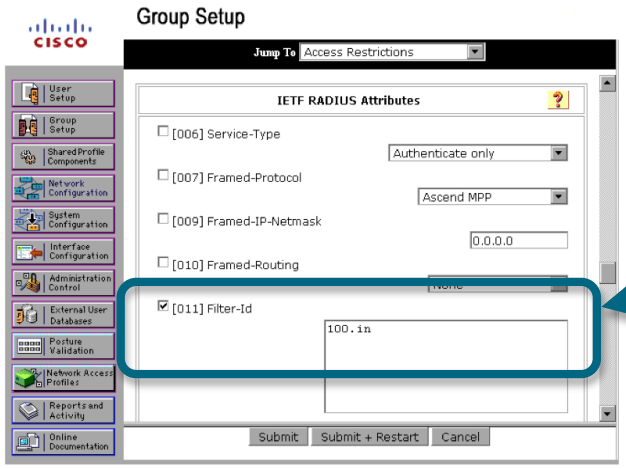
```
switch(config)#ip access-list extended 100
switch(config-ext-nacl)#deny ip any 10.100.60.0
0.0.0.255
switch(config-ext-nacl)#deny tcp any host 10.100.10.116
eq www
switch(config-ext-nacl)#permit ip any any
```

Define a numbered ACL that will be applied to the port when a user authenticates. Make a note of this number ("100") as you will need it when defining the Filter-Id tag on the ACS.

With Filter-IDs, the switch must be preconfigured with each ACL that could be dynamically applied to the port. If there are 5 groups of users with 5 unique policies, then there will be 5 ACLs configured on the switch. Only numbered ACLs from 1 to 199 or 1300 to 2699 are supported.

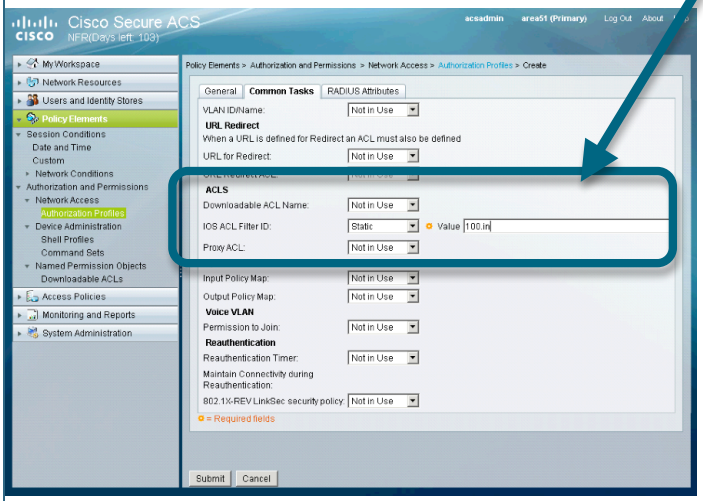
AAA RADIUS Server Configuration Examples

ACS 4.2 Example



For Filter-IDs, the AAA RADIUS Server (e.g., ACS) must be configured to use the RADIUS Filter-ID Attribute [011] instead of the Cisco VSA. The Filter-ID Attribute will be set to the name of an ACL on the switch with the suffix ".in" (indicating it should be applied in the inbound direction).

ACS 5.1 Example



Filter-ID ACL—Offer a distributed method of group-to-policy mapping. In this mode, the full definition of the identity-based ACLs resides on the switch. The authentication server determines the user's group or authorization profile and the identifier (the Filter-ID) of the ACL that should be applied to that user. The authentication server sends the Filter-ID to the switch as an attribute in the RADIUS Access-Accept message. The switch matches the Filter-ID to a locally-configured ACL that has the same number as the Filter-ID (e.g., Filter-ID=101 will match up to access-list 101). That ACL is then applied to the port. Because the access-list elements are defined on the switch, filter-ID ACLs allow for local variation in policy. Because of the distributed nature of Filter-IDs, a configuration management tool should be used to ensure centralized management and change control.

ACLs (Additional Resources)

For more detailed information on Identity and ACLs please refer to the Baseline Access-List (ACL) Deployment Guide:
http://wwwin.cisco.com/ios/tech/ibns/docs/aclauth_EDCS-632761-2-25-08.pdf

(Optional) Authorization – Centrally Administered (continued)

Dynamic VLAN Assignment

Switch Configuration

Example ACCESS VLAN

```
switch(config)#vlan 60
switch(config-vlan)#name ACCESS
```

By dynamically assigning VLAN values to switch ports based on the client's authenticated identity, the network maintains the ability to group users per administrative policy. This allows the notion of groups and group-applicable policy profiles to be carried down to the networking level.

Create the required L2 VLANs—For multi-layer access designs, these VLANs must be trunked up to the distribution-layer switches where the corresponding VLANs are defined, together with the corresponding VLAN interfaces (these two steps are not shown in the configuration sample below). For routed access designs, it is instead required to define the L2 VLANs as well as the VLAN interfaces

Note: There are three options for dynamic VLAN Assignment (this example only shows the use of dynamic VLAN assignment by NAME)

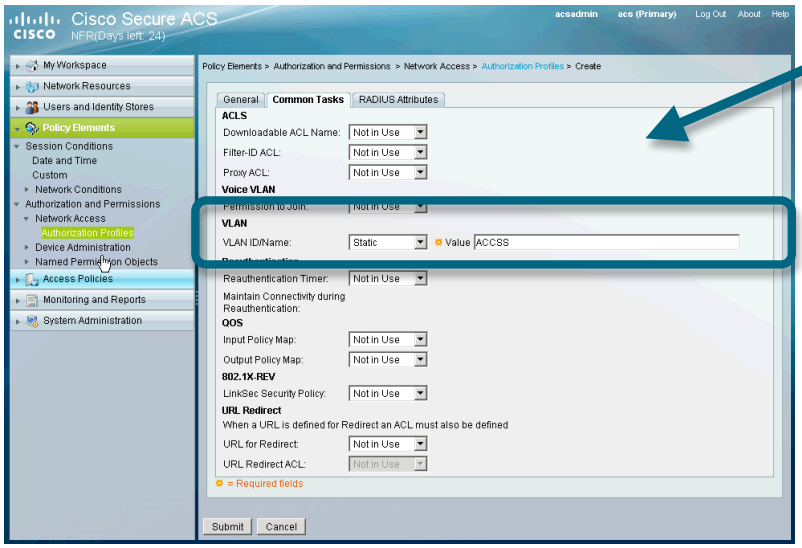
Dynamic VLAN Assignment by Number

Dynamic VLAN Assignment by Name

Dynamic VLAN Assignment by Group (aka User Distributioin)

AAA RADIUS Server Configuration Examples

ACS 5.1 (Dynamic VLAN by NAME = (ACCESS)



Here we have applied the vlan named ACCESS to this particular named Authorization Profile which has been named CorpUser. This Authorization Profile is now available for use with the 802.1X or MAB Access Services.

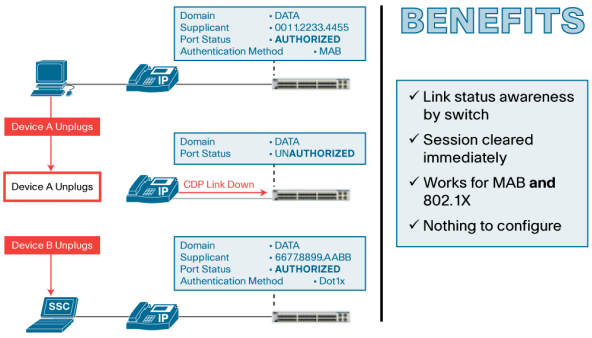
IP Telephony Integration (Interface commands relevant to IP telephony deployments)

Authentication

`switch(config-if)# authentication host-mode multi-domain`
 	
`switch(config)# vlan vlan-id`
`switch(config-vlan)# name VOICE`
 	
`switch(config-if)# switchport voice vlan vlan-id`
	Multi-Domain Authentication (MDA) host mode allows an IP phone and a PC to authenticate on the same switch port while it places them on appropriate voice and data VLANs. Allows both a host and a voice device, such as an IP phone (Cisco or non Cisco), to be authenticated on an 802.1x-authorized or MAB-enabled port. Note: You must configure the voice VLAN for the IP phone when the host mode is set to multidomain mode.
	Note: In order for the phone to be placed into the voice VLAN, you **must** specify the cisco-av-pair as device-traffic-class=voice on your AAA RADIUS server. This is configured in ACS in the Authorization Profiles.
	Note: This feature is recommended over the predecessor 802.1X VVLAN with Cisco Discovery Protocol Bypass, as this feature requires authentication either through IEEE 802.1X or MAC Authentication Bypass for the phone, rather than the less secure Cisco Discovery Protocol discovery and autoconfiguration.

Legacy VVID CDP Bypass
 	
`switch(config-if)# switchport voice vlan vlan-id`
`switch(config-if)# authentication port-control auto`
`switch(config-if)# authentication host-mode single`
`switch(config-if)# dot1x pae authenticator`
	(Optional) By default, enabling the voice VLAN and 802.1x on an interface port enables Cisco Discovery Protocol Bypass if the host mode is set to single (which is the default).
	Note: Preferred and recommended is to enable MDA rather than Cisco Discovery Protocol Bypass.

Optional IPT Usability Enhancements

`switch(config-if)# errdisable detect cause security-violation shutdown vlan-id`	(Optional) You use the voice-aware 802.1x security feature on the switch to disable only the VLAN on which a security violation occurs, whether it is a data or voice VLAN. You can use this feature in IP phone deployments where a PC is connected to the IP phone. A security violation found on the data VLAN results in the shutdown of only the data VLAN. The traffic on the voice VLAN flows through the switch without interruption.
`switch(config-if)# errdisable recovery cause security-violation`	(Optional) Enables automatic per VLAN error recovery
Cisco Discovery Protocol Enhancement for Second Port Disconnect 	This advanced Cisco IBNS feature is automatically enabled when using the following or later software releases: • Catalyst 6500: Cisco IOS Software 12.2(33)SXI • Catalyst 4500: Cisco IOS Software 12.2(50)SG • Catalyst 3xxx/2xxx: Cisco IOS Software 12.2(50)SE • IP Phone firmware: 8.4(1)

Identity Enabled Cisco IP Phones

Phones	EAP-MD5	EAP-TLS	EAP-FAST	EAP-Logoff
Cisco Third Generation* 7906, 7911, 7931, 7941, 7961, 7970, 7942, 7945, 7962, 7965, 7975 devices	Yes Firmware 7.2(3) +	Yes Firmware 8.5(2) + Requires Cisco Unified Communications Manager 7.1(2)*	Yes Firmware 8.5(2) + Requires Cisco Unified Communications Manager 7.1(2)*	Yes Firmware 7.2(3) +

Cisco IP Phone models prior to Cisco's third generation do not support X.509 certificates (for example, 7902, 7905, 7910, 7912, 7920, 7935, 7936, 7940 and 7960) and therefore have no road map to support IEEE 802.1X.

Using EAP-TLS on phones in conjunction with ACS 5.x, it is possible to perform touchless deployment of 802.1X.

Using both manufacturing (MIC) and locally significant certificates (LSC) in a two-stage model enables a touchless and secure deployment mode.

*Cisco Unified Communications Manager 7.1.2 is required if you want to be able to globally enable 802.1X (instead of manually, on the phone itself) from the Cisco Unified Communications Manager GUI. However the 802.1X phone firmware works with earlier versions of Cisco Unified Communications Manager.

Optional Local WebAuth (Switch Configurations for Local Web Authentication as a Fallback to 802.1X or MAB)	
You have the option of using web-based authentication as a fallback authentication method to 802.1X or MAB	
Global Configuration Additions	
switch(config)# ip access-list extended DEFAULT-ACCESS switch(config-ext-nacl)#remark Allow DCHP switch(config-ext-nacl)#permit udp any any eq bootps switch(config-ext-nacl)#remark Allow DNS switch(config-ext-nacl)#remark Allow HTTP switch(config-ext-nacl)#permit tcp any any eq www switch(config-ext-nacl)#remark Allow HTTPS switch(config-ext-nacl)#permit tcp any any eq 443 switch(config-ext-nacl)#remark Allow ICMP for test purposes switch(config-ext-nacl)#permit icmp any any switch(config-ext-nacl)#remark Implicit Deny switch(config-ext-nacl)#deny ip any any switch(config-ext-nacl)#end	Sample ACL to be used by the WebAuth profile
switch(config)# **line console 0** switch(config-line)# **login authentication** list-name	Use the following to prevent you from locking yourself out of console access after enabling AAA authentication for the default group RADIUS. List-name is user defined.
switch(config)#**aaa authentication login default group radius**	Defines RADIUS as the authentication method for WebAuth
switch(config)#**aaa authentication login** list-name none	Excludes line console from AAA authentication
switch(config)#**aaa authorization auth-proxy default group radius**	
switch(config)#**radius-server attribute 8 include-in-access-request**	Makes it possible for a network access device (NAD) to provide the RADIUS server with a hint of the user IP address in advance of user authentication.
switch(config)#**ip admission name** LOCAL-WEBAUTH **proxy http**	Global configuration command to enable web authentication
switch(config)#**ip device tracking**	Enables the IP device tracking table, which is required for web-based authentication
switch(config)# **ip http server**	Enables the HTTP server. The web-based authentication feature uses the HTTP server to communicate with the hosts for user authentication.
switch(config)# **ip http secure-server**	Enables the HTTPS server on the switch
switch(config)# **fallback profile** WEB-AUTH	Defines a fallback profile to allow an 802.1x port to authenticate a client by using WebAuth
switch(config-fallback-profile)# **ip access-group** DEFAULT-ACCESS in	Applies an ACL to the fallback profile
switch(config-fallback-profile)# **ip admission** LOCAL-WEBAUTH	Applies the WebAuth IP admission rule/profile proxy HTTP to the desired/specified interfaces
Switch Port Configuration Additions	
switch(config-if)# **no authentication event no-response**	Ensures that **authentication event no-response** is disabled
switch(config-if)# **authentication fallback** WEB-AUTH	Enables WebAuth as a fallback to 802.1X or MAB
Authorization Profile on AAA Server (Must return this in the access ACCEPT)	
cisco-av-pair equals priv-lvl=15	This must be set in the RADIUS Attributes of your AAA authorization profile.

(Optional) Customized WebAuth Pages	
Preparation	
Modify the custom pages and copy them to your switch storage media (see example below): **Copy ftp:**//anonymous:anonymous@10.1.10.10/Directory/customLogin_Page.htm **{bootflash: | flash:}** **copy ftp:**//anonymous:anonymous@10.1.10.10/Directory/customAuthSuccess_Page.htm **{bootflash: | flash:}** **copy ftp:**//anonymous:anonymous@10.1.10.10/Directory/customAuthFailed_Page.htm **{bootflash: | flash:}** **copy ftp:**//anonymous:anonymous@10.1.10.10/Directory/customSessionExpired_Page.htm **{bootflash: | flash:}**	Use a simple HTML editor, for example, PageBreeze HTML Editor at http://www.pagebreeze.com/. It maintains everything in the htm file (no directories and so on). Note: Depending on the hardware platform, you have the option of storing these files on either the bootflash or flash drives.
(Optional) Global Configuration – Customized WebAuth Pages (Bootflash Example)	
switch(config)# **ip admission proxy http login page file bootflash:**customLogin_Page.htm switch(config)# **ip admission proxy http login expired page file bootflash:**customSessionExpired_Page.htm switch(config)# **ip admission proxy http success page file bootflash:**customAuthSuccess_Page.htm switch(config)# **ip admission proxy http failure page file bootflash:**customAuthFailed_Page.htm	Add these commands to the global configuration in this specific order to enable your customized pages.

WebAuth (Specific Show Commands)	
Show commands to help verify application of dCALs	
switch(config)# **show ip admission configuration**	Used to verify the configuration of custom authentication proxy web pages

Useful Show Commands (Configuration Verification and Troubleshooting)	
Authentication	
switch# **show authentication sessions** [interface-id]	Displays the summary of all Auth Manager sessions; optionally you can specify a desired interface to gain more information about the authentication and authorization state of that interface.
switch# **show dot1x interface interface**-id details	To display the system dot1x capabilities, protocol version, and timer values, use the show **dot1x** command. Legacy command, deprecated by **show authentication session**.
switch# **show errdisable detect**	Displays the current settings of the errdisable timeout feature and, if any of the ports are currently error disabled, the reason that they are error disabled.
switch# **show ip device tracking all** switch# **show epm session ip** local-host-ip-address switch# **show ip access-list interface** {ingress pacl or dACL name}	Displays the IP device tracking table that contains the host IP addresses learned through ARP or DHCP. Using the IP address learned from the IP device tracking table show command above, specifies the IP address as the required option for the show epm session ip command to verify whether the dACL was successfully downloaded from ACS Displays the contents of the inbound and outbound IP access list applied to the specified interface. In addition to verifying the PACL or dACL applied to the port, this command also shows the ACL statistics (number of matches displayed next to the ACL lines) that are kept and displayed per interface.
switch# **show tcam interface** interface-id **acl in ip**	Used to display interface-based TCAM information. Unfortunately this is only useful on the Catalyst 6500 to determine the dACL/ACE entries applied.

802.1X Default Settings	
Feature	**Default Setting**
Authentication, authorization, and accounting (AAA)	Disabled
RADIUS server • IP address • UDP authentication port • Key	 • None specified • 1645 • None specified
Per interface 802.1X protocol enable state	Force-authorized The port transmits and receives normal traffic without 802.1X-based authentication of the client.
Periodic reauthentication	Disabled
Time between reauthentication attempts	3600 sec (1 hour)
Quiet period	60 sec (1 minute) Number of seconds that the switch remains in the quiet state following a failed authentication exchange with the client.
Retransmission time	30 sec Number of seconds that the switch should wait for a response to an EAP request/identity frame from the client before retransmitting the request.
Maximum retransmission number	2 Number of times that the switch sends an EAP request/identity frame before restarting the authentication process.
Multiple host support	Disabled
Client timeout period	30 sec When relaying a request from the authentication server to the client, the amount of time that the switch waits for a response before retransmitting the request to the client.
Authentication server timeout period	30 sec When relaying a response from the client to the authentication server, the amount of time that the switch waits for a reply before retransmitting the response to the server. This setting is not configurable.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV
Amsterdam, The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

Printed in USA C27-574041-00 2/10