TOMORROW starts here.

cisco

Cisco live!

Identity Based Networking: IEEE 802.1X and Beyond

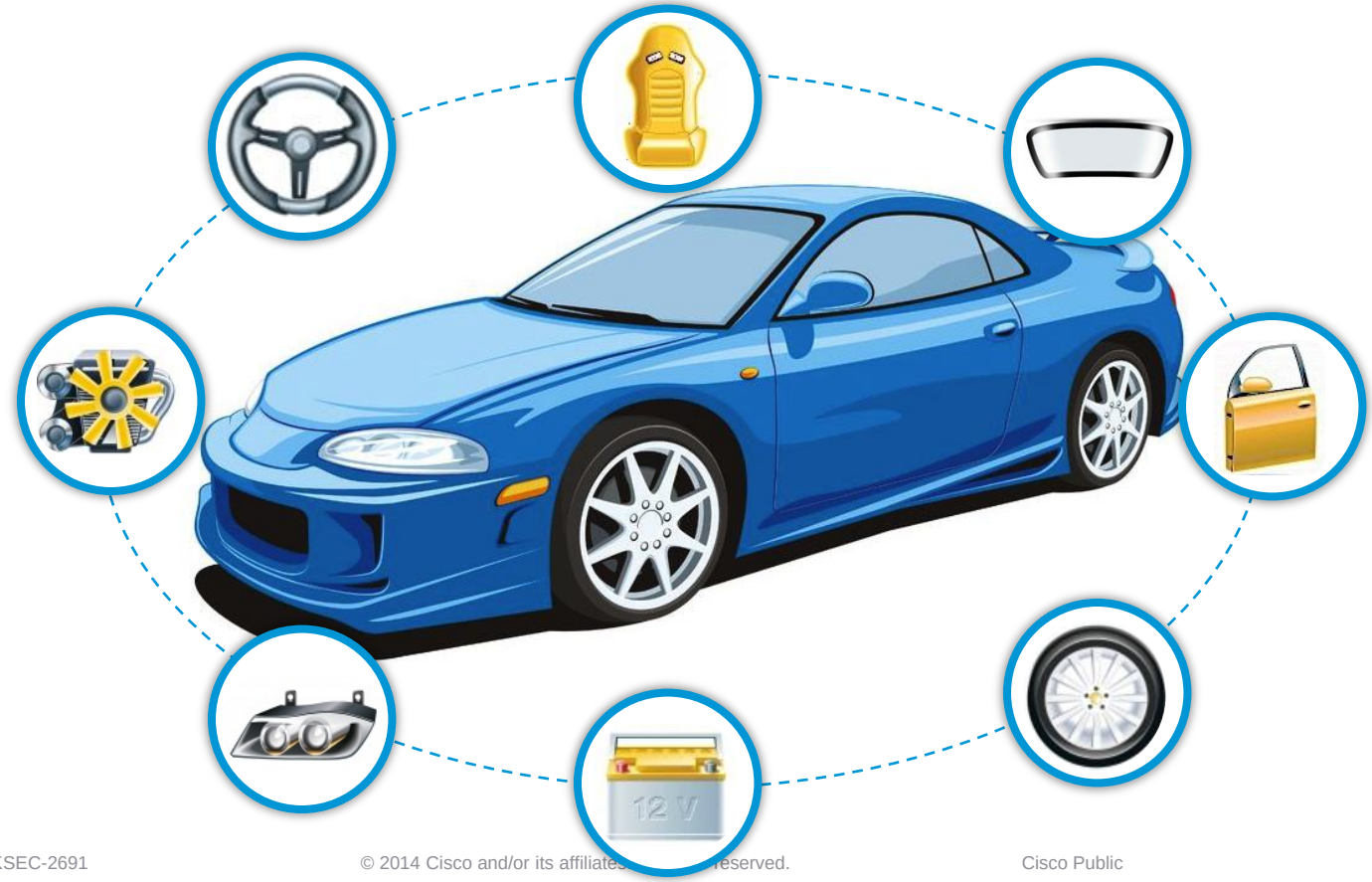
BRKSEC-2691

Hariprasad Holla

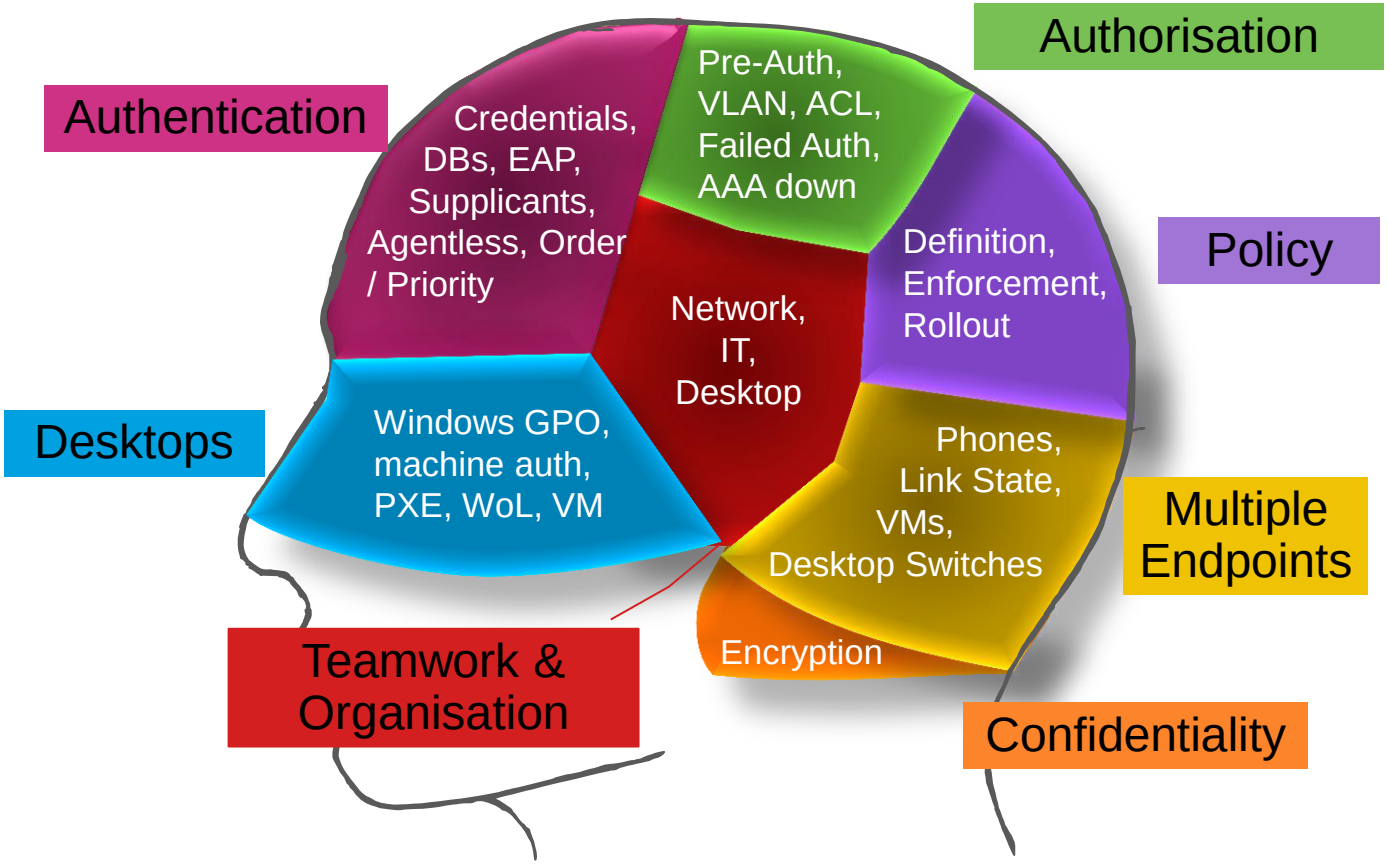
Technical Marketing Engineer

Cisco live!

Distinct Parts that Make up a System



Think Identity: Think System



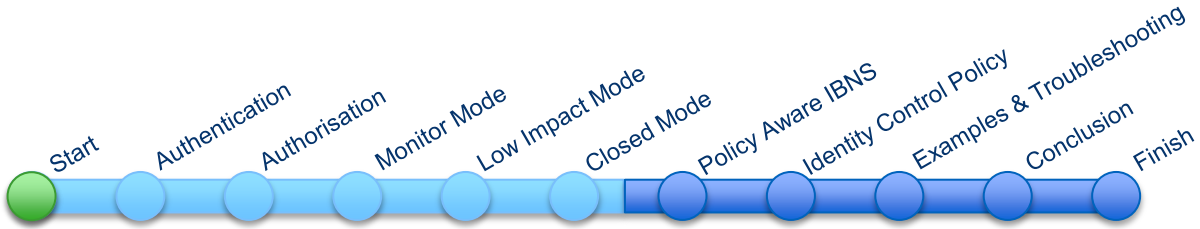
Agenda

- **Deployment Considerations**
  - Authentication
  - Authorisation
- **Deployment Scenarios**
  - Monitor Mode
  - Low Impact Mode
  - Closed Mode
- **IOS Identity Evolution**
  - Policy Aware IBNS
  - Policy Model (Identity Control Policy)
  - Examples & Troubleshooting

For Your Reference

Real World Example

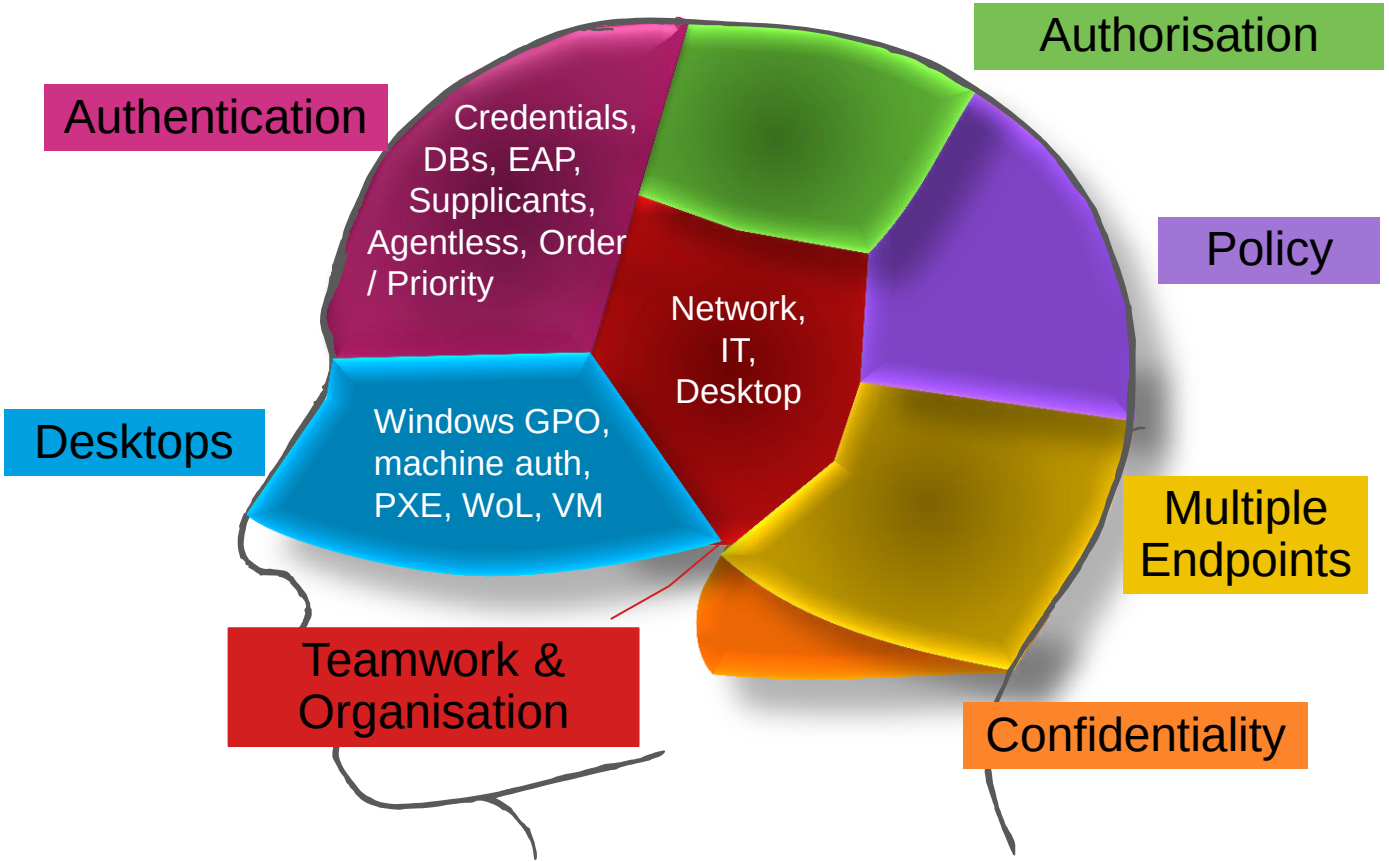
ISE
(Identity Services Engine)



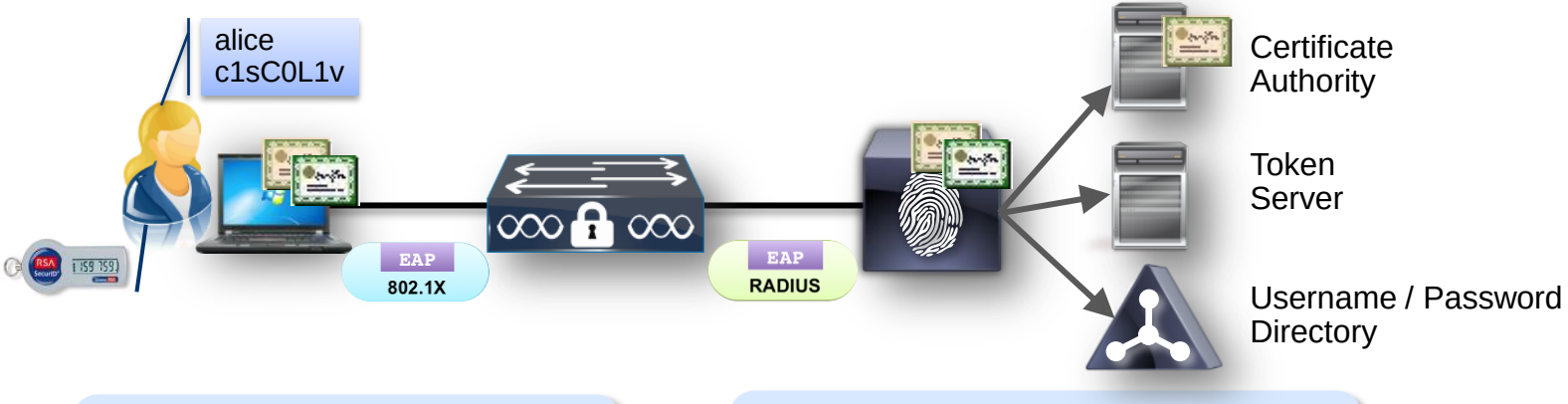



Deployment Considerations
Authentication

Thinking About Authentication



Choosing Credentials for 802.1X



Common Types

- Passwords
- Certificates
- Tokens

Deciding Factors

- Security Policy
- Validation
- Distribution & Maintenance

Deployment Best Practices

Re-use Existing Credentials

Understand the Limitations of Existing Systems

How To Submit Credentials

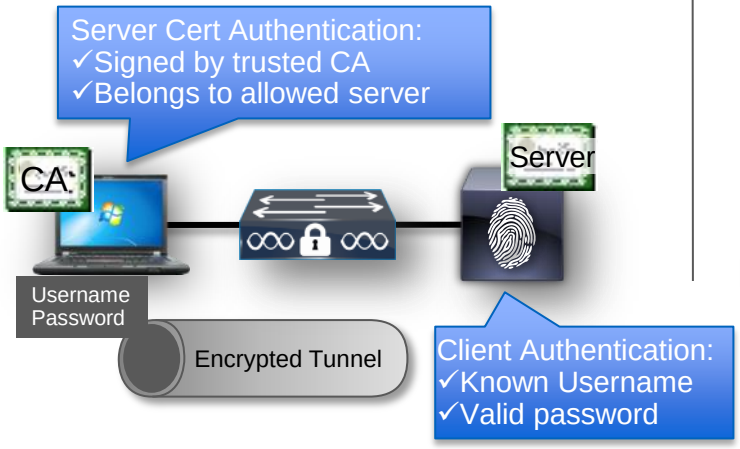
Mutual Authentication

- Server must validate client's identity **and vice versa**

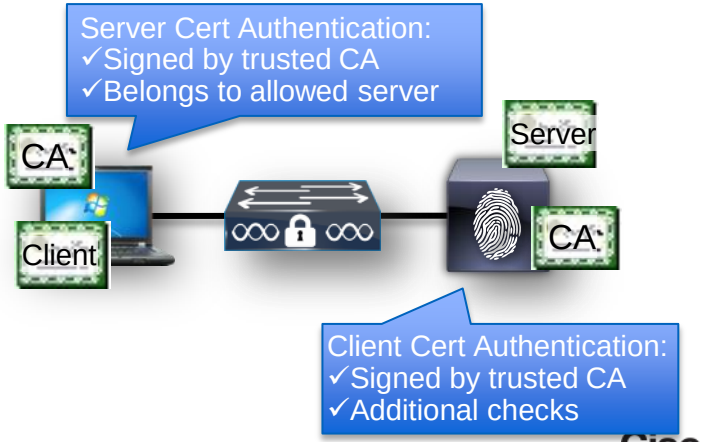
Security

- Client credentials cannot be snooped or cracked.

PEAP-MSCHAPv2

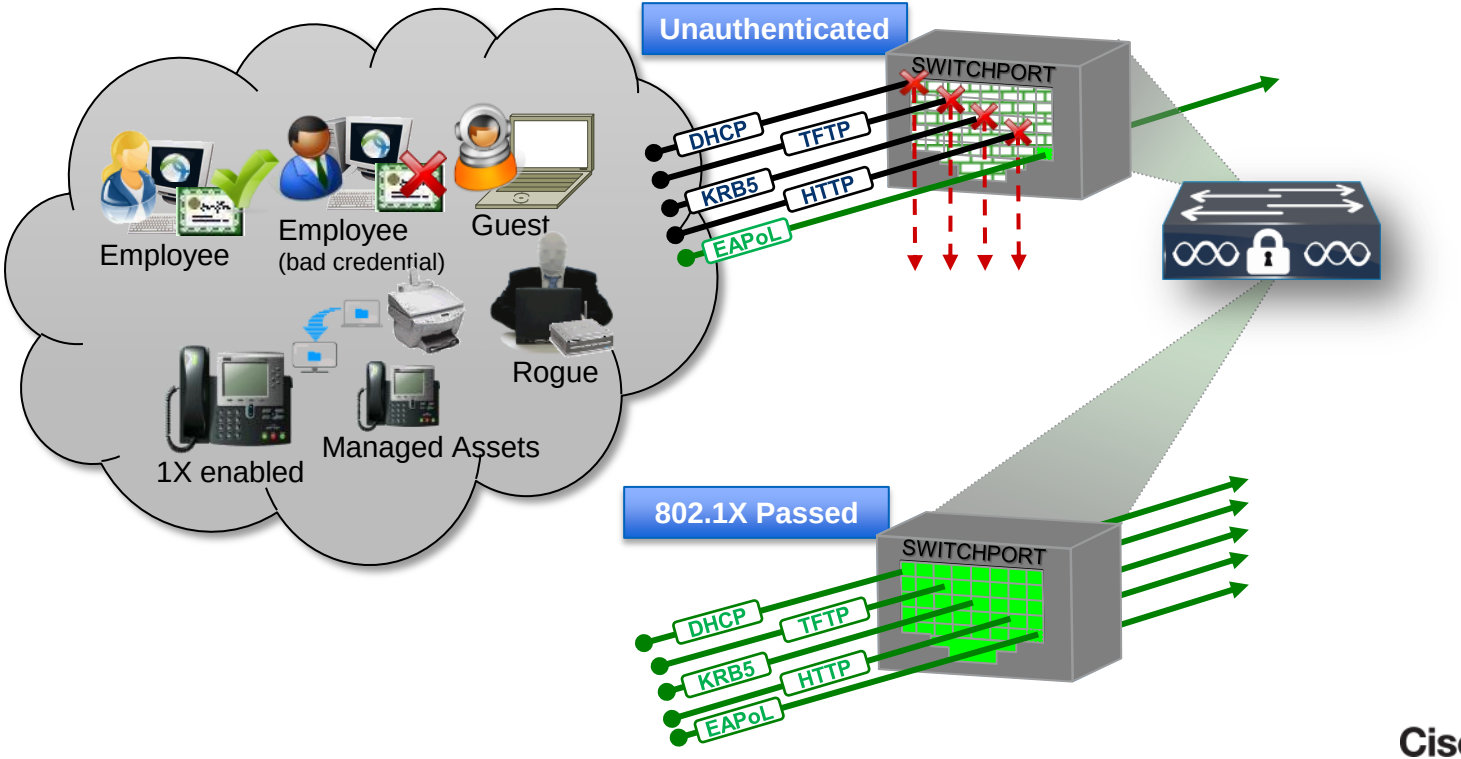


EAP-TLS



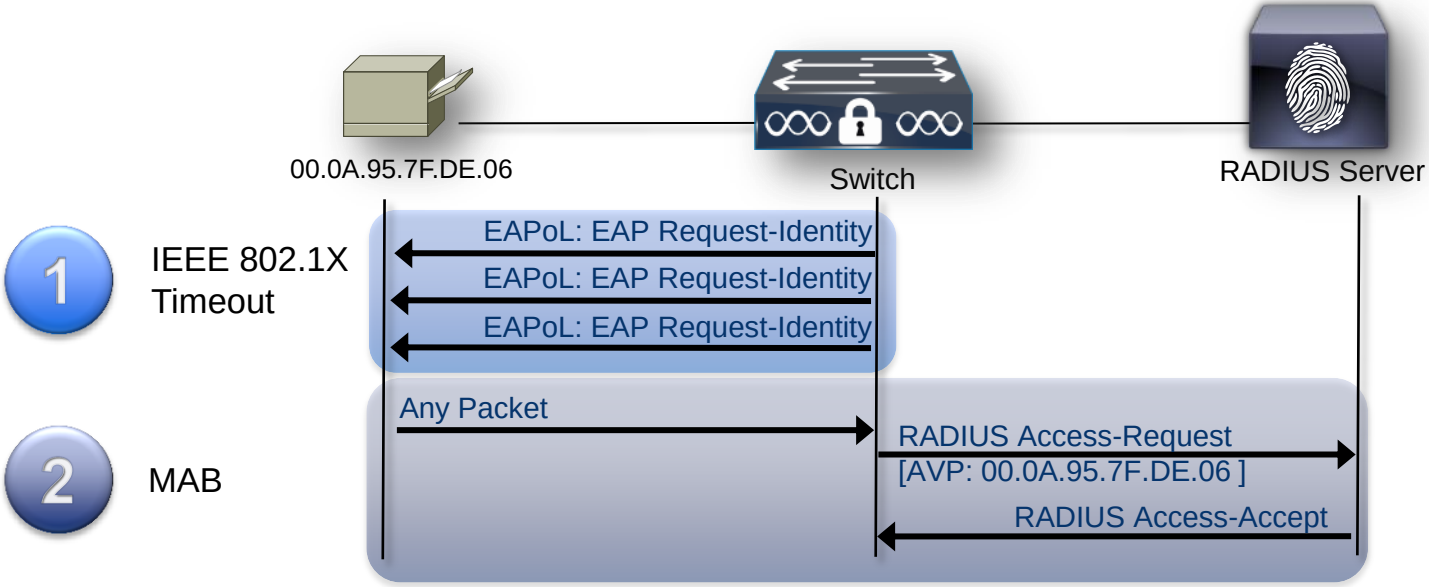
Real Networks Can't Live on 802.1X Alone

Default Access Control is Binary



MAC Authentication Bypass (MAB)

“Authentication” for Clientless Devices



IEEE 802.1X with MAB

MAB enables differentiated access control

MAB leverages centralised policy on AAA server

Dependency on IEEE 802.1X timeout → delayed network access

- Default timeout is 30 seconds with three retries (90 seconds total)
- 90 seconds > DHCP timeout.

MAB requires a database of known MAC addresses

Three Options For MAB-Related Delays

1

Change the Timeout

```
interface GigabitEthernet1/4
 dot1x max-reauth-req 2
 dot1x timeout tx-period 30
```

Short Enough To Prevent Timeouts
Long Enough To Allow 802.1X Devices to Authenticate

802.1X → Timeout → MAB

(max-reauth-req + 1) * tx-period

2

"FlexAuth"

```
interface GigabitEthernet1/4
 authentication order mab dot1x
 authentication priority* dot1x mab
```

MAB → MAB Fails → 802.1X

Prepare For Additional Control Plane Traffic

First packet from device will trigger MAB

3

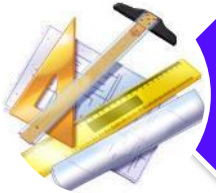
Low Impact Deployment Scenario

*Priority Matters! www.cisco.com/go/ibns → Whitepapers

MAC Databases: Device Discovery

Find It

- Leverage Existing Asset Database
- e.g. Purchasing Department, CUCM



Build It

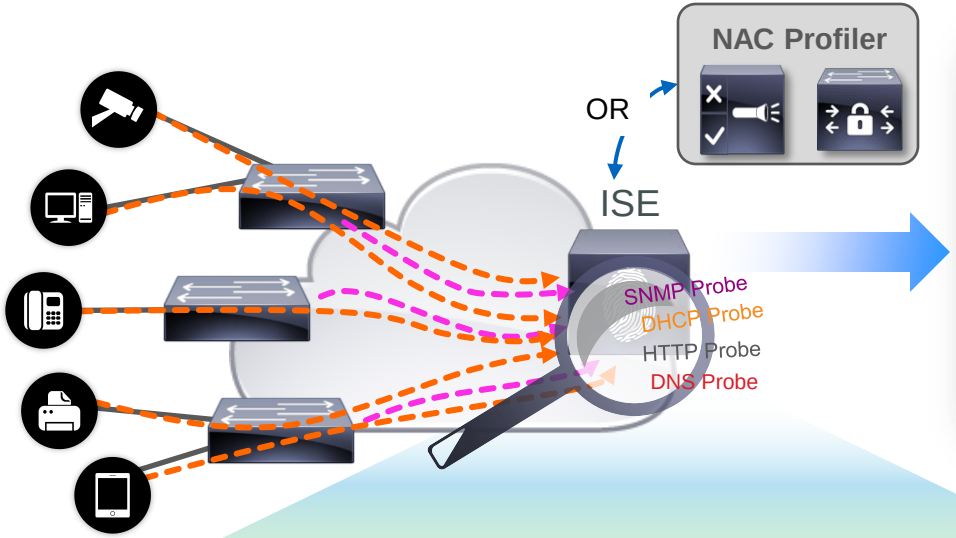
- Bootstrap methods to gather data
- e.g. SNMP, Syslog, Accounting

Buy It

- Automated Device Discovery
- e.g. ISE

Building Your MAB Database

Profiling Tools Are Evolving



Endpoints

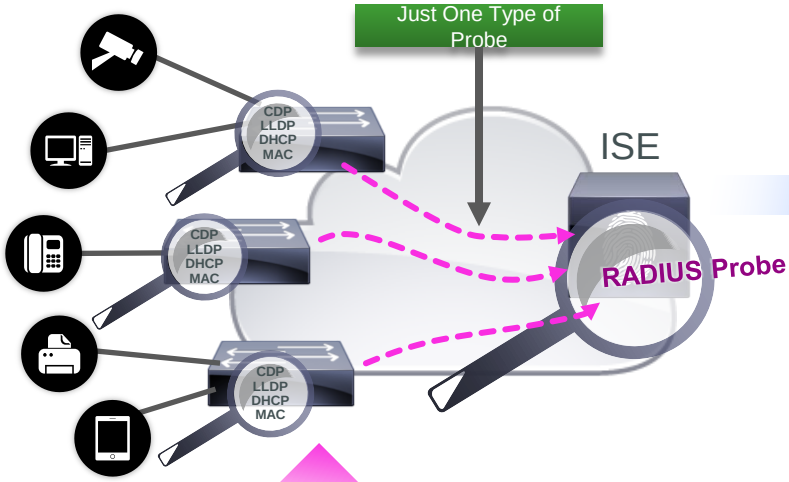
Edit | Create | Delete | Import

Endpoint Profile	MAC Address
Apple_iPad	1C:17:D3:4A:34:43
Apple_iPad	1C:BD:B9:D7:9F:9E
Cisco-Access-Point	54:75:D0:AB:91:E1
Cisco-IP-Phone-7945	00:22:90:5A:DF:D0
Cisco-WLC-2100-Series	54:75:D0:5F:91:80
ISE-Appliance	00:50:56:B4:00:1C

Probe-Gathered Information	+	Profile Conditions	=	PROFILED
Example: MAC OUI + Lexmark		If DHCP Class ID Contains E260dn		It's a Lexmark E260n Printer

Building Your MAB Database

Profiling Tools Are Evolving



Endpoints

Edit | Create | Delete | Import

Endpoint Profile	MAC Address
Apple_iPad	1C:17:D3:4A:34:43
Apple_iPad	1C:BD:B9:D7:9F:9E
Cisco-Access-Point	54:75:D0:AB:91:E1
Cisco-IP-Phone-7945	00:22:90:5A:DF:D0
Cisco-WLC-2100-Series	54:75:D0:5F:91:80
ISE-Appliance	00:50:56:B4:00:1C

Device Sensor
15.0(1)SE1
ISE 1.1

BRKSEC-2044 "Building an Enterprise Access Control Architecture with ISE"
BRKSEC-3045 "Advanced ISE and Secure Access Deployment"

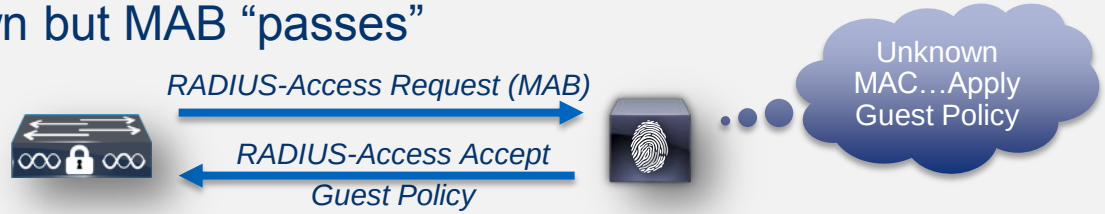
To Fail or Not to Fail MAB?

Two Options for Unknown MAC Addresses

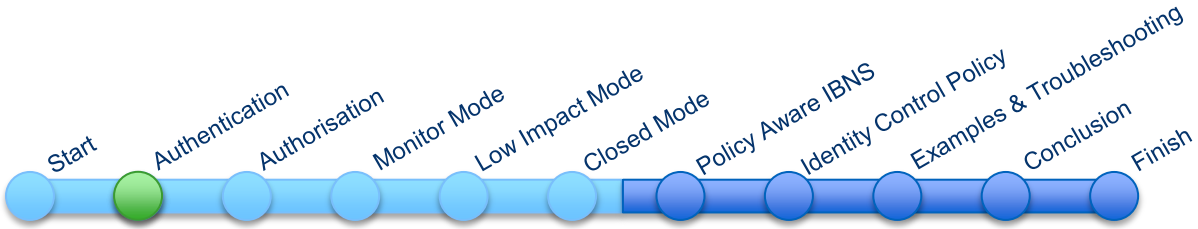
1 MAB Fails – control of session passes to switch

1) No Access
2) Switch-based Web-Auth
3) Guest VLAN

2 MAC is Unknown but MAB "passes"



- AAA server determines policy for unknown endpoints (e.g. network access levels, re-auth policy)
- Good for centralised control & visibility of guest policy (VLAN, ACL)

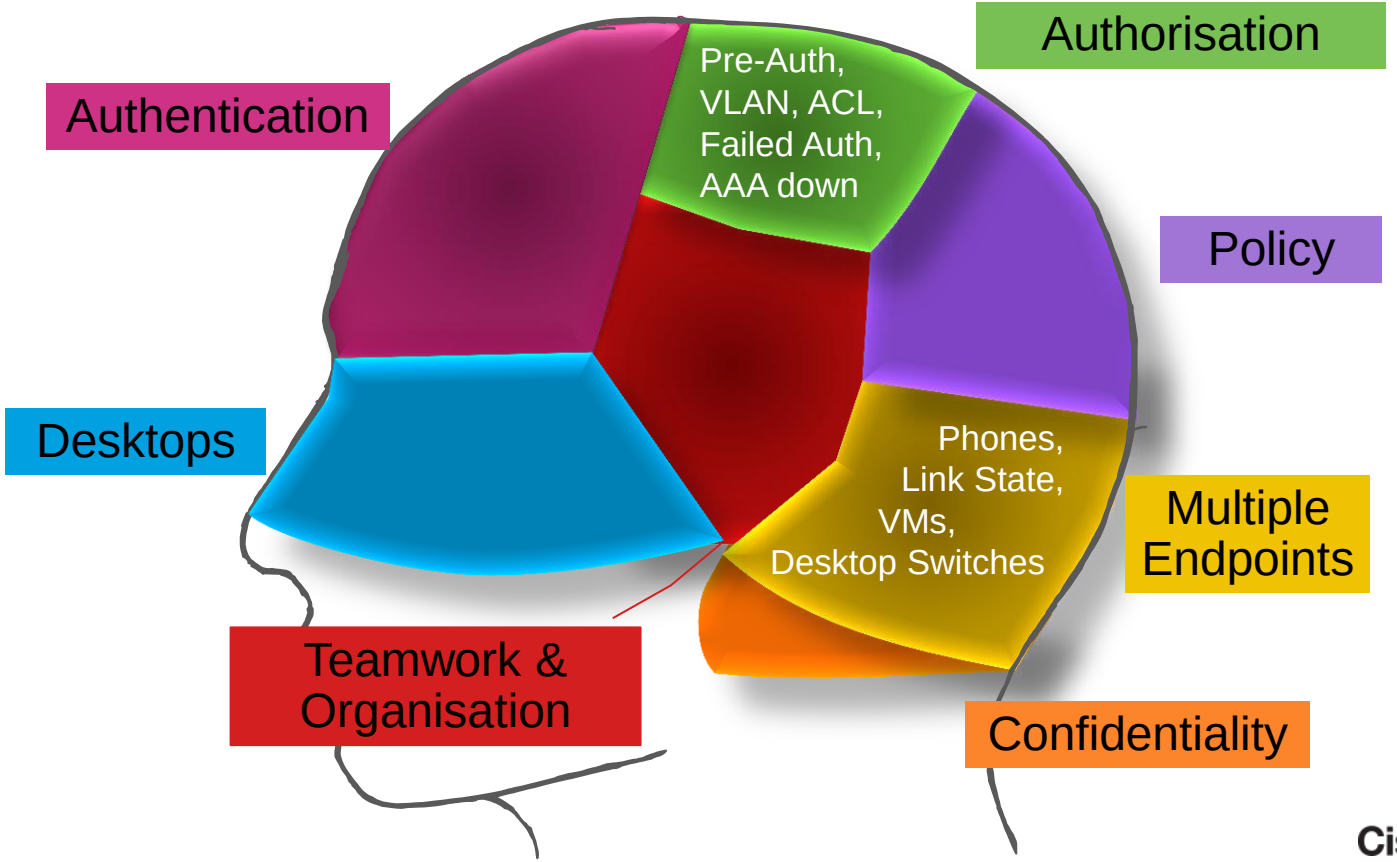




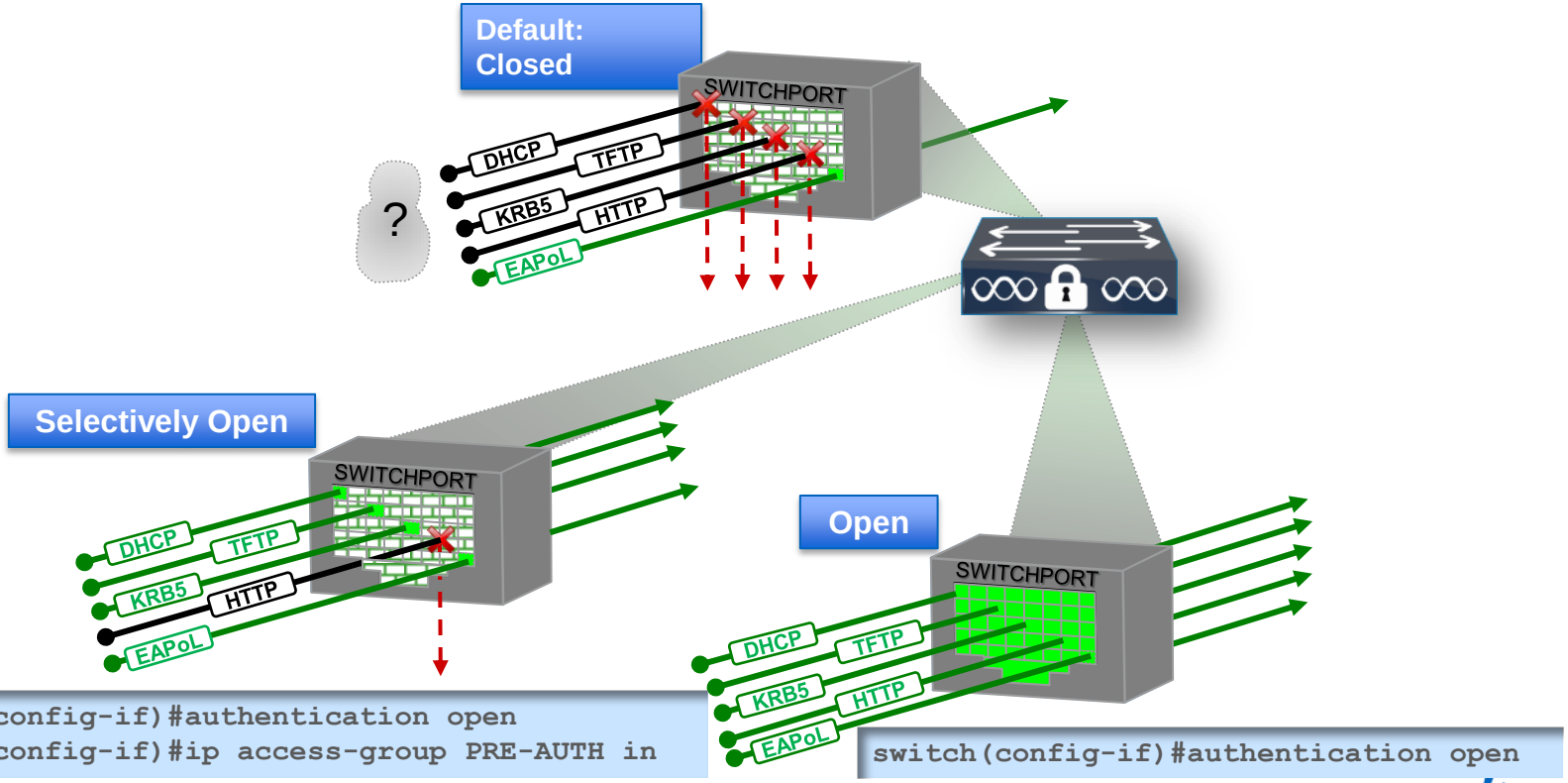

Deployment Considerations

Authorisation

Thinking About Authorisation



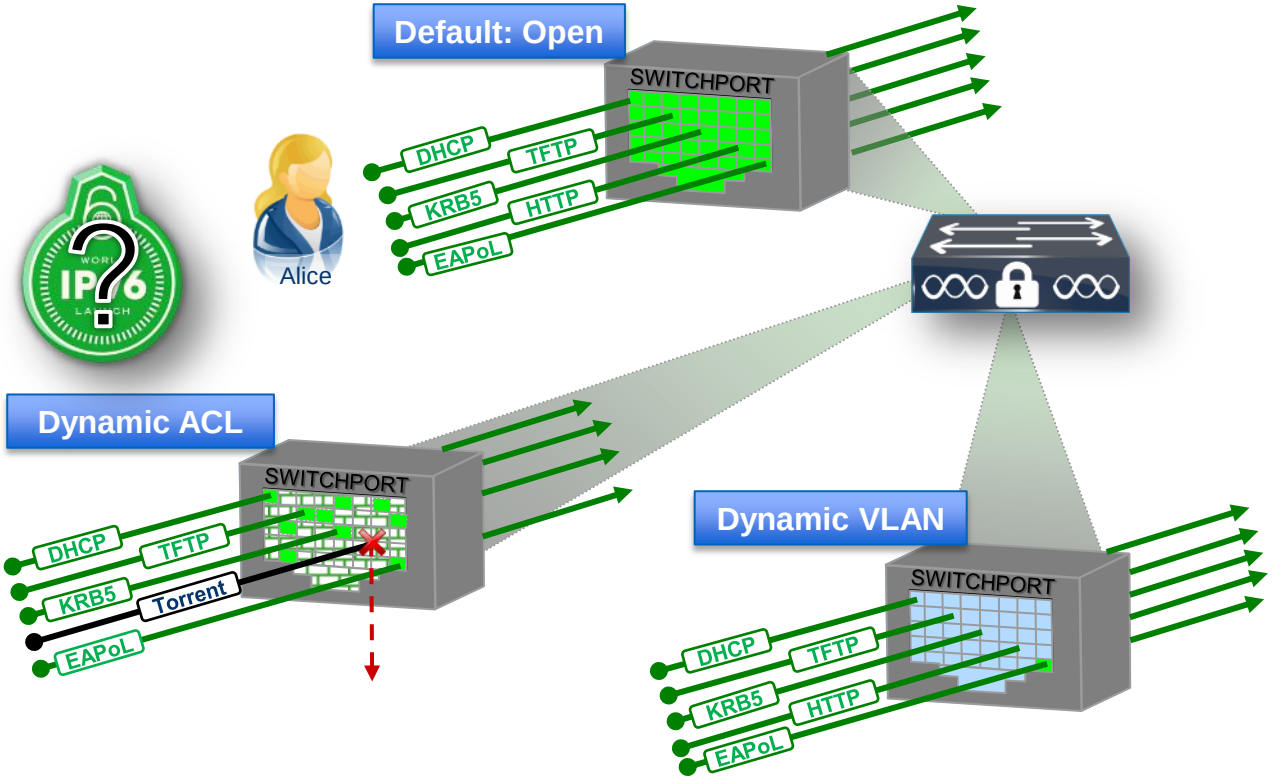
Authorisation Options: Pre-Authentication



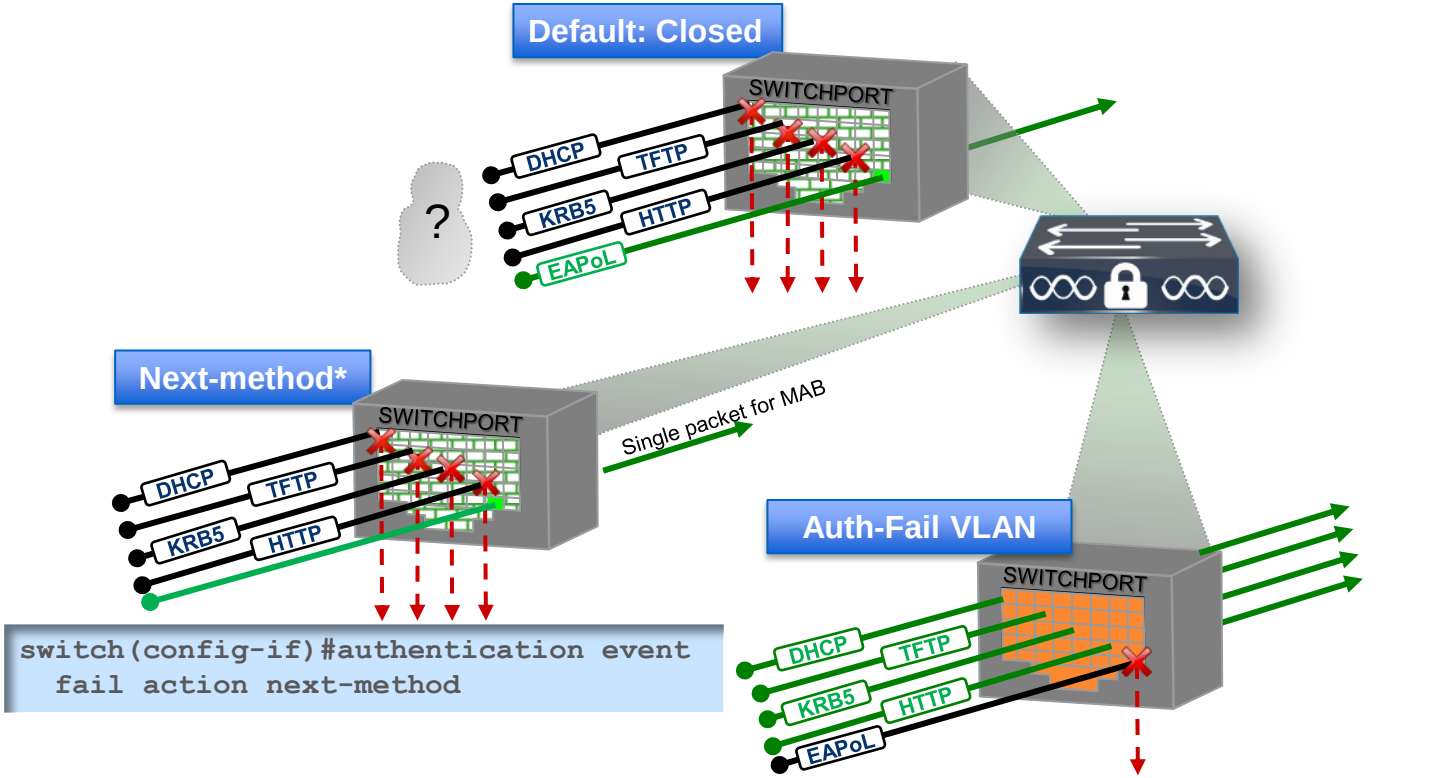

```
switch(config-if)#authentication open
switch(config-if)#ip access-group PRE-AUTH in
```

```
switch(config-if)#authentication open
```

Authorisation Options: Passed Authentication



Authorisation Options: Failed 802.1X

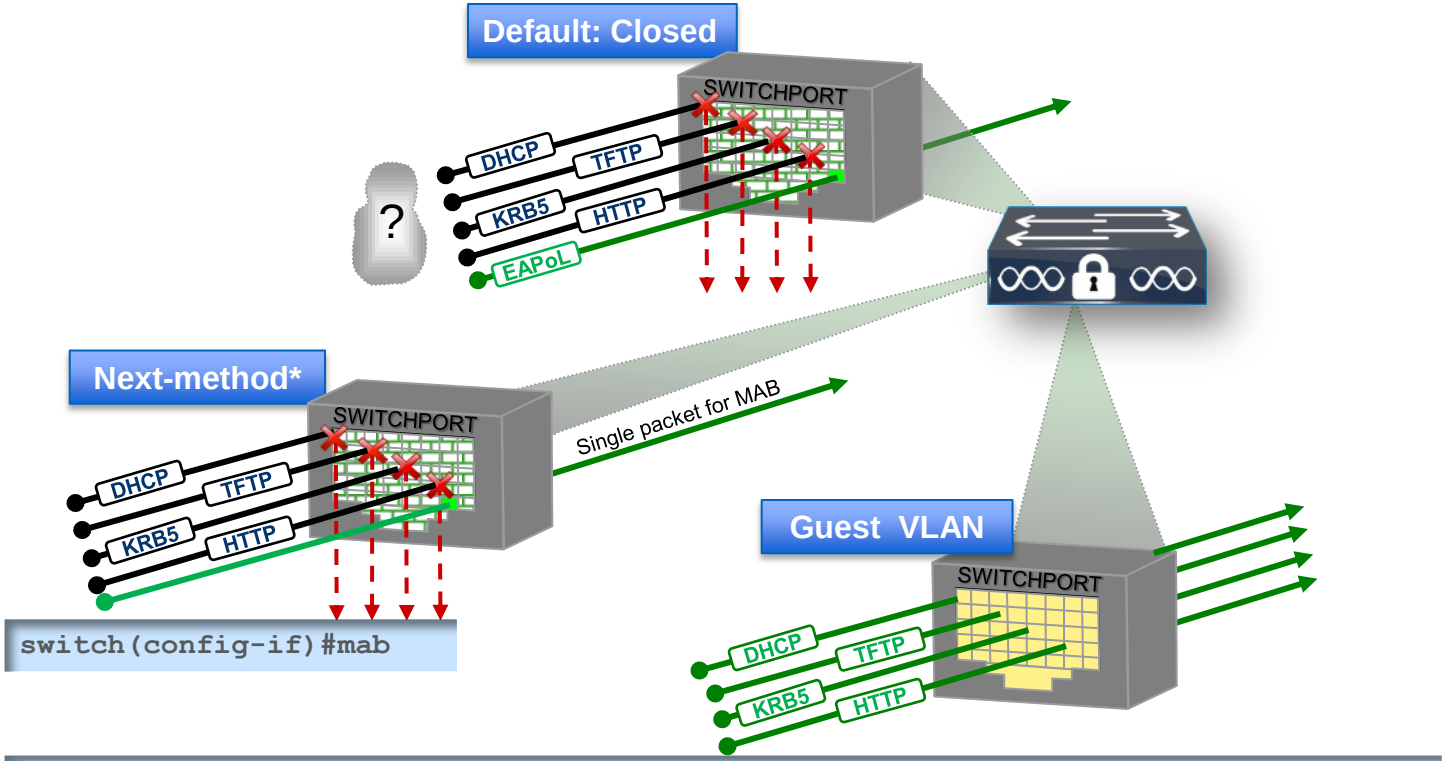



```
switch(config-if)#authentication event
  fail action next-method
```

```
switch(config-if)#authentication event
  fail action authorize vlan 50
```

*Final authorisation determined by results of next method

Authorisation Options: No Client

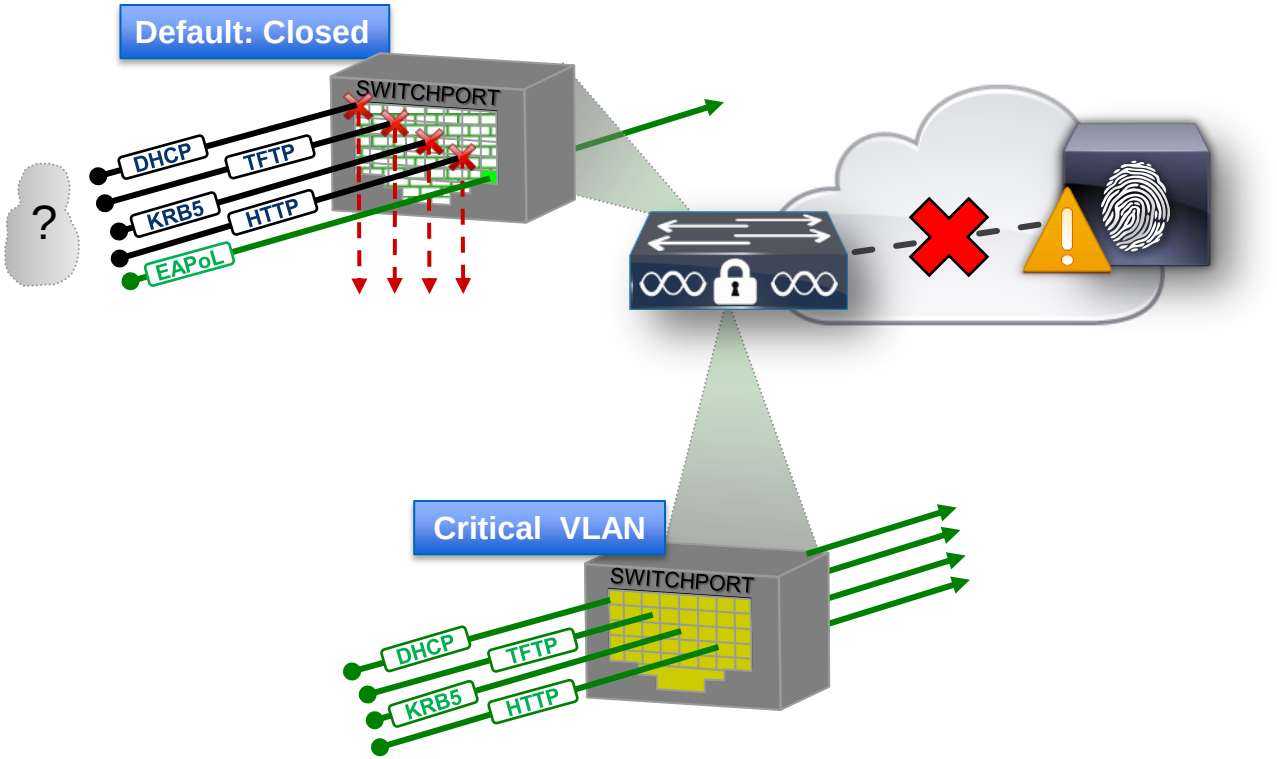



```
switch(config-if)#mab
```

```
switch(config-if)#authentication event no-response action authorize vlan 51
```

*Final authorisation determined by results of next method

Authorisation Options: AAA Server Dead

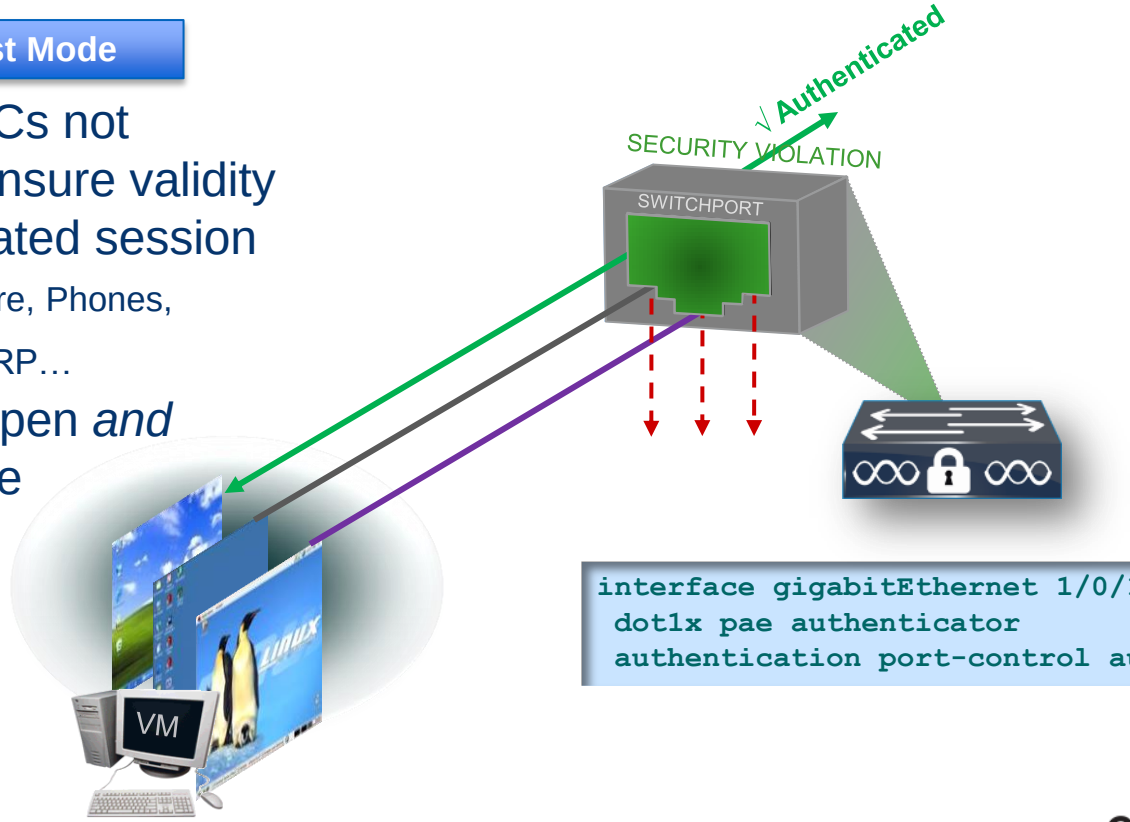



```
switch(config-if)# authentication event server dead action authorize vlan 52
```

Authorisation: Single MAC Filtering

Default: Single Host Mode

- Multiple MACs not allowed to ensure validity of authenticated session
  - Hubs, VMware, Phones, Gratuitous ARP…
- Applies in Open *and* Closed Mode




```
interface gigabitEthernet 1/0/1
 dot1x pae authenticator
 authentication port-control auto
```

Modifying Single-MAC Filtering For IP Phones

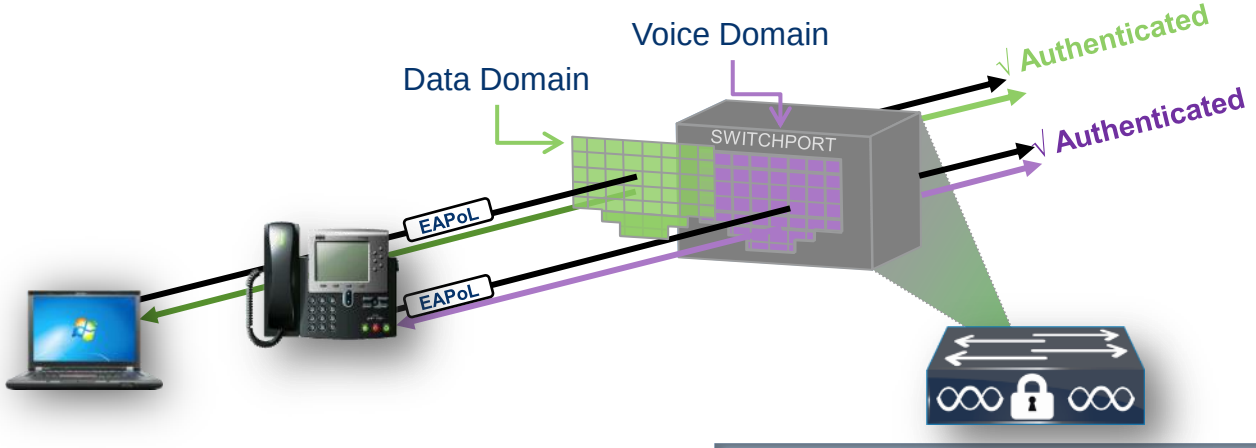
Multi-Domain Authentication (MDA) Host Mode

IEEE 802.1X

Single device per port

MDA

Single device *per domain* per port



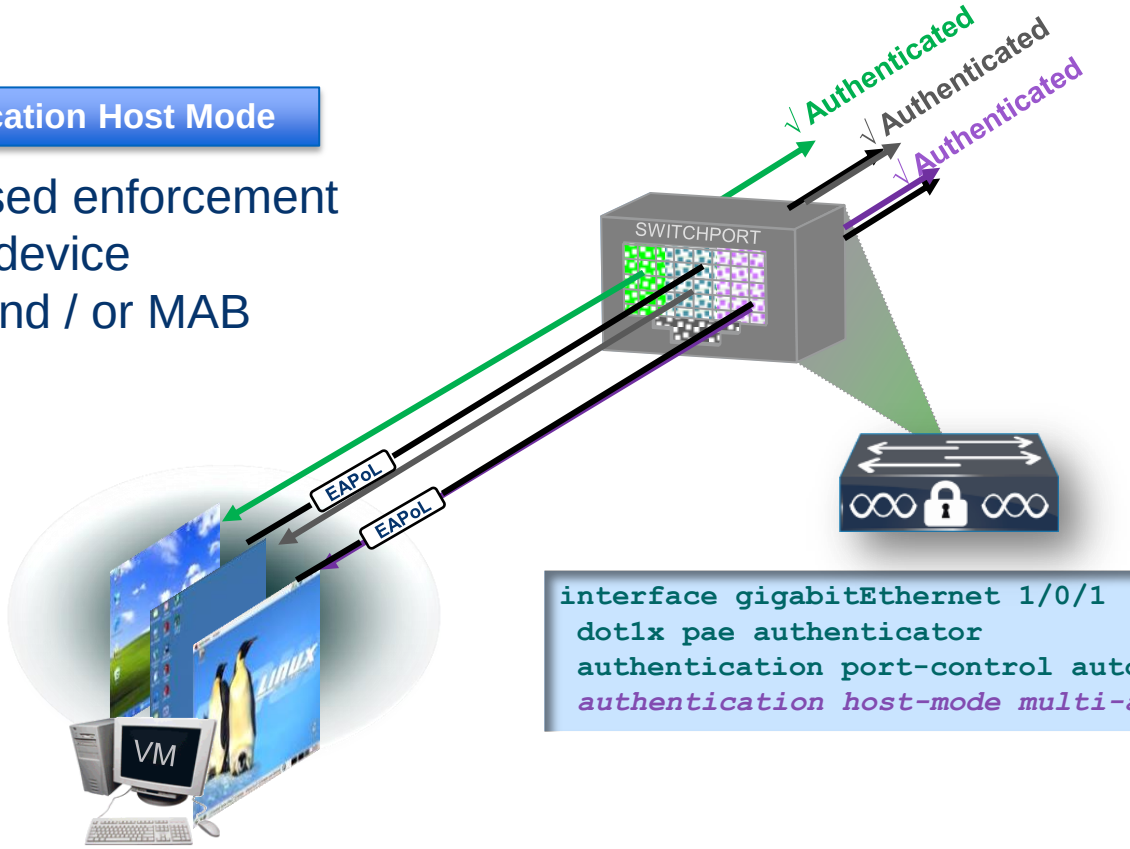
- MDA replaces CDP Bypass
- Supports Cisco & 3rd Party Phones
- Phones *and* PCs use 802.1X or MAB

```
interface gigabitEthernet 1/0/1
 dot1x pae authenticator
 authentication port-control auto
 authentication host-mode multi-domain
```

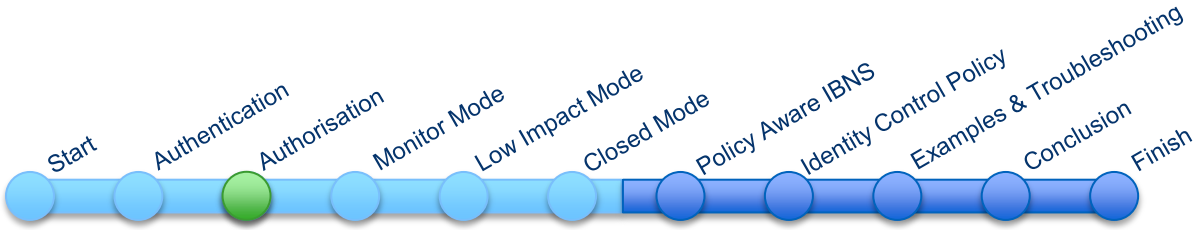
Modifying Single-MAC Filtering For Virtualised Endpoints

Multi-Authentication Host Mode

- MAC-based enforcement for each device
- 802.1X and / or MAB



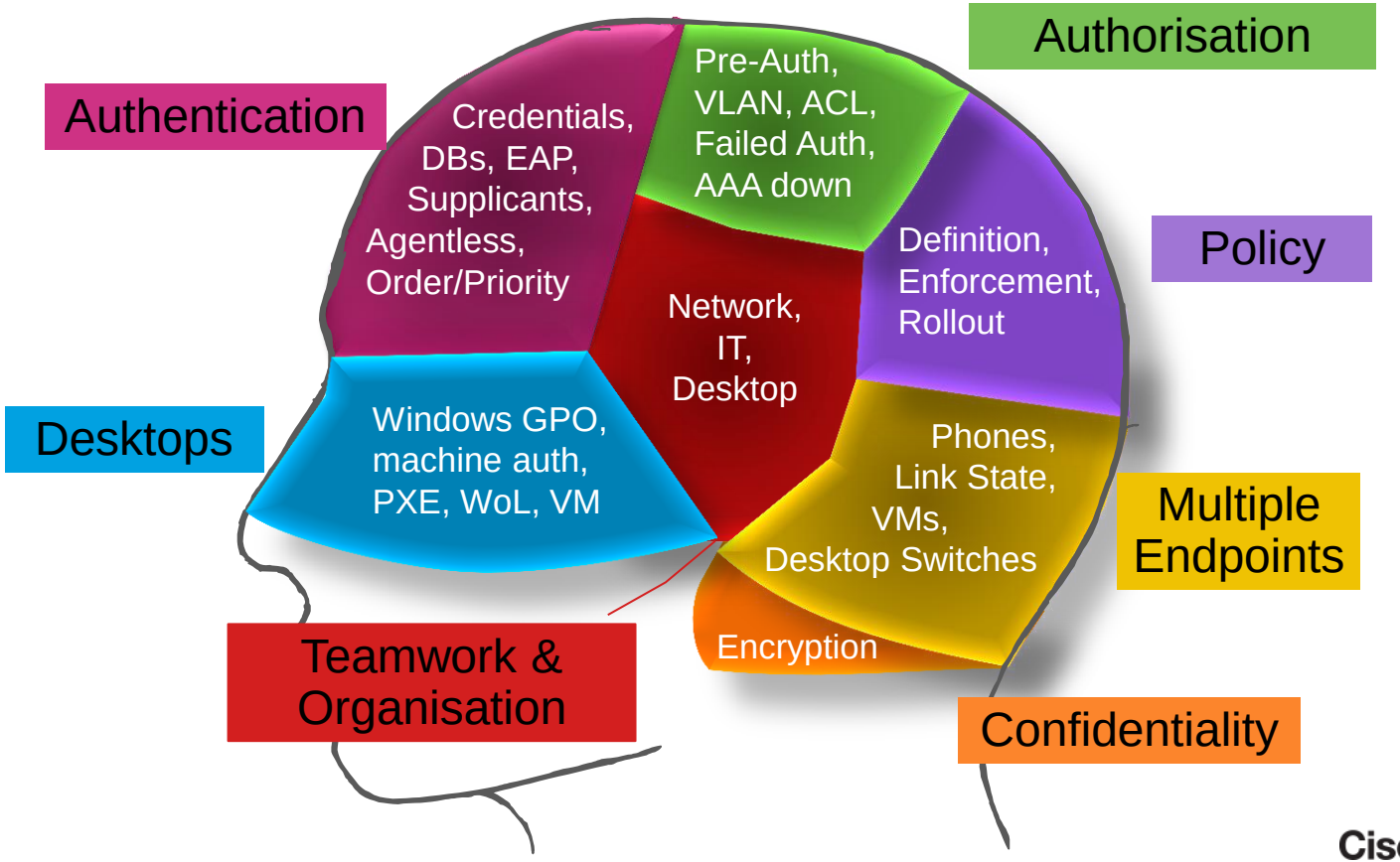

```
interface gigabitEthernet 1/0/1
 dot1x pae authenticator
 authentication port-control auto
 authentication host-mode multi-auth
```






Implementing Phased Deployments
‘Monitor Mode’

Thinking About Deployment Scenarios



Enabling 802.1X!

@Company XYZ

IT Manager

I've done my homework in Proof of concept Lab and it looks good. I'm turning on 802.1X tomorrow..

Enabled 802.1X

I can't connect to my network. It says Authentication failed but I don't know how to fix. My presentation is in 2 hours…

Increased help desk calls

- Deploying 802.1X needs careful study of the network
- Needs to be done in phases; non-disruptive way!

Three Proven Deployment Scenarios

Monitor Mode

- Authentication without Access Control

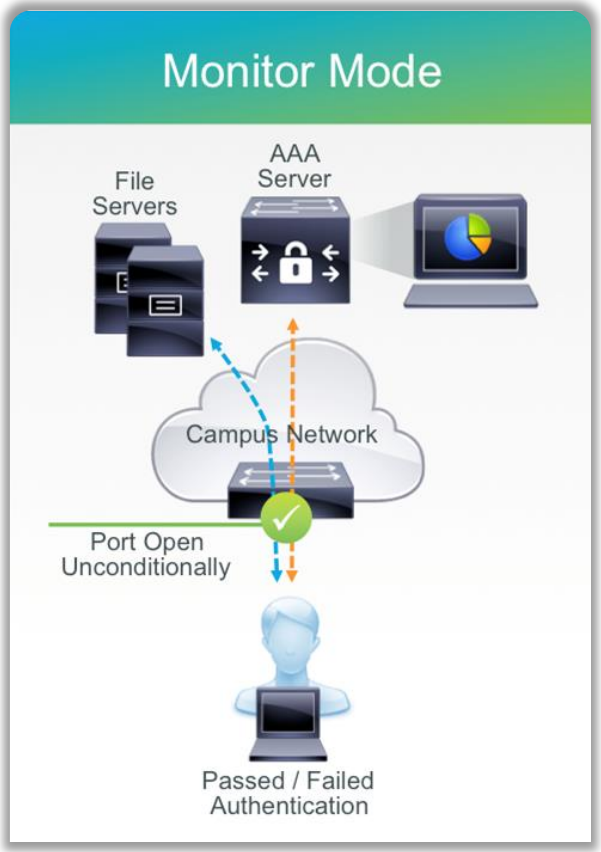
Low Impact Mode

- Minimal Impact to Network and Users

Closed Mode

- Logical Isolation
- Formerly “High Security”

Scenario 1: Monitor Mode Overview



Monitor Mode Goals

- No impact to existing network access
- See… - What is on the network
  - Who has a supplicant
  - Who has good credentials
  - Who has bad credentials
- Deterrence through accountability

Monitor Mode: How To

- Enable 802.1X and MAB
- Enable Open Access
  - All traffic in addition to EAP is allowed
  - Like not having 802.1X enabled except authentications still occur
- Enable Multi-Auth host mode
- **No Authorisation**

Monitor Mode

Switch Configuration Example

Switch Global Config

```
aaa new-model
aaa authentication dot1x default group radius
aaa authorization network default group radius
aaa accounting dot1x default group radius
radius-server host 10.100.10.150 auth-port 1812 acct-port 1813 key
cisco
radius-server vsa send authentication
authentication mac-move permit
```

Switch Interface Config

```
interface GigabitEthernet1/4
   switchport access vlan 60
   switchport mode access
   switchport voice vlan 61
   authentication host-mode multi-auth
   authentication open
   authentication port-control auto
   mab
   dot1x pae authenticator
   authentication violation restrict
```

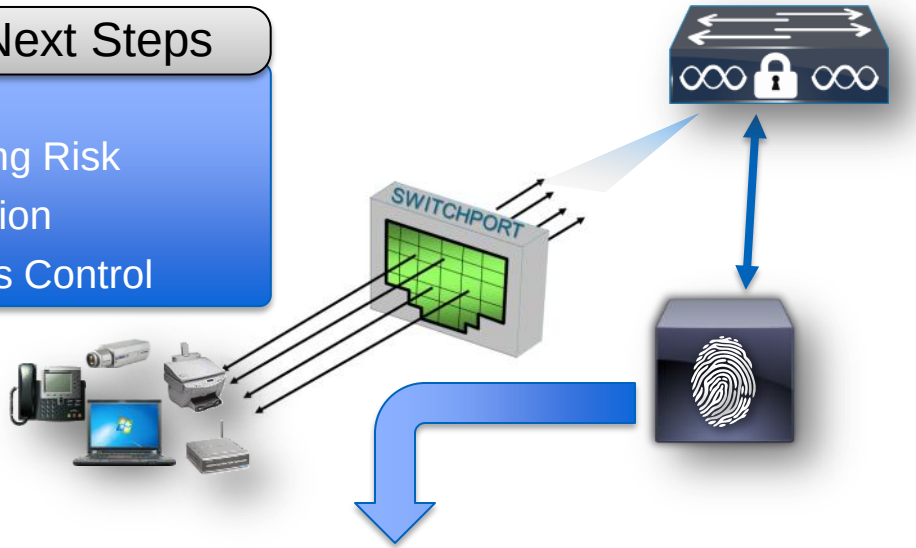
Monitor Mode

Basic 802.1X/MAB

Monitor Mode: Next Steps

Monitor Mode Next Steps

- Improve Accuracy
- Evaluate Remaining Risk
- Leverage Information
- Prepare for Access Control

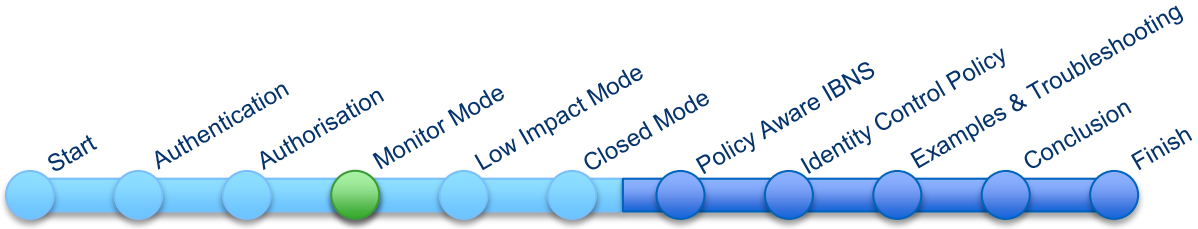


RADIUS Authentication & Accounting Logs

- Passed / Failed 802.1X
  (Who has bad credentials? Misconfigurations?)
- Passed / Failed MAB attempts
  (What don't I know?)

Monitor Mode In a Nutshell

Summary	• Authentication without Authorisation
Benefits	• Extensive Network Visibility • No Impact to Endpoints or Network
Limitations	• No Access Control
Next Steps	• Monitor the Network • Evaluate Remaining Risk • Prepare for Access Control

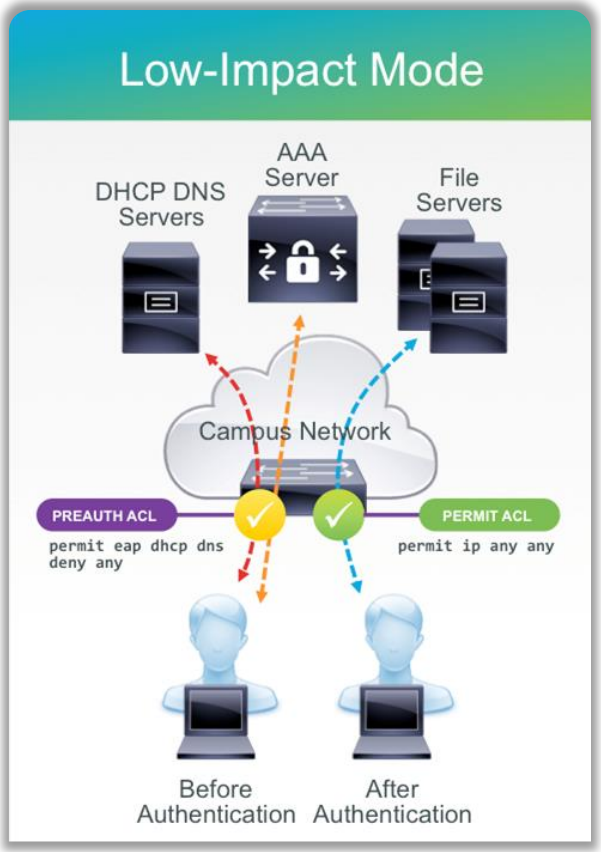





Implementing Phased Deployments

‘Low Impact Mode’

Scenario 2: Low Impact Mode



Low-Impact Mode Goals

- Begin to control / differentiate network access
- Minimize Impact to Existing Network Access
- Retain Visibility of Monitor Mode
- “Low Impact” == no need to re-architect your network
  - Keep existing VLAN design
  - Minimize changes

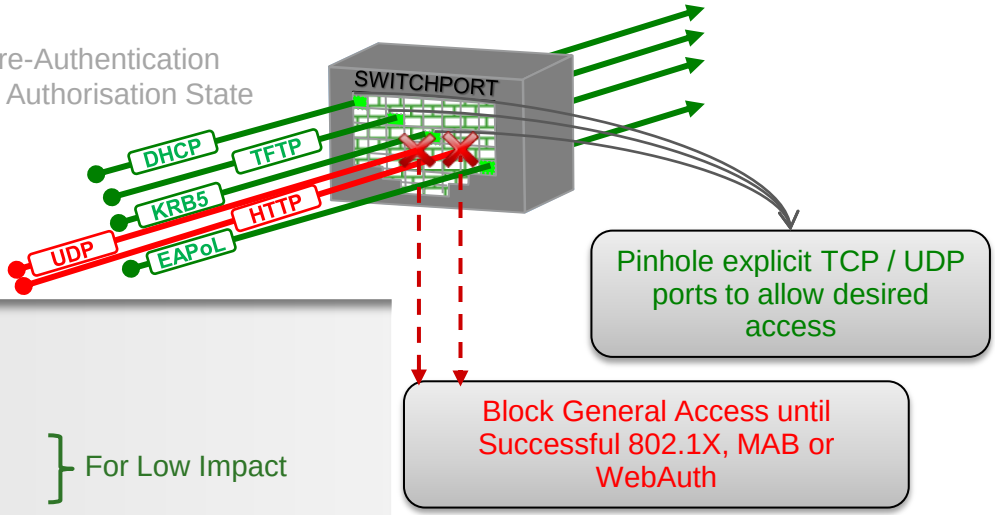
Low-Impact Mode: How To

- Start from Monitor Mode
- Add ACLs, dACLs and flex-auth
- Limit number of devices connecting to port
- Authorise phones with dACLs and Voice VSA

Low Impact Mode: Switch

Switch Global Config (add to Monitor Mode)

```
ip device-tracking
```



Switch Interface Config

```
interface GigabitEthernet1/4
 switchport access vlan 60
 switchport mode access
 switchport voice vlan 61
 ip access-group PRE-AUTH in
 authentication open
 authentication port-control auto
 mab
 dot1x pae authenticator
 authentication violation restrict
```

For Low Impact

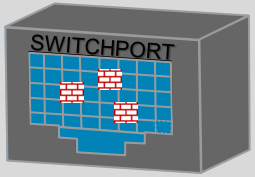
From Monitor Mode

Pre-Auth ACL Considerations

Approach 1: Selectively block traffic

Selectively protect certain assets / subnets
Low risk of inadvertently blocking wanted traffic

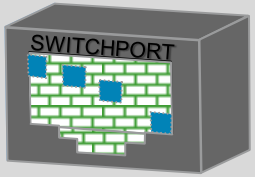
Example: Block unauthenticated users from Finance servers



Approach 2: Selectively allow traffic

More secure, better control
May block wanted traffic

Example: Only allow pre-auth access for PXE devices to boot



- Pre-auth port ACL is arbitrary and can progress as you better understand the traffic on your network
- Recommendation: use least restrictive ACL that you can; time-sensitive traffic is a good candidate for ACL.

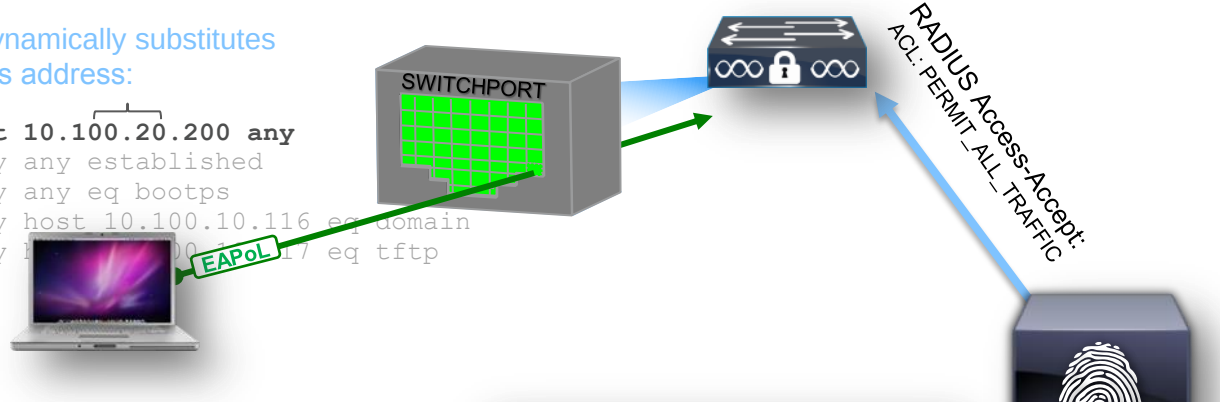
Low Impact Mode: AAA Server

Configure Downloadable ACLs for Authenticated Users

Switch dynamically substitutes endpoint's address:

Pre-Auth ACL

```
permit ip host 10.100.20.200 any
permit tcp any any established
permit udp any any eq bootps
permit udp any host 10.100.10.116 eq domain
permit udp any h[illegible]00.1[illegible]17 eq tftp
```



- Contents of dACL are arbitrary
- Can have as many unique dACLs as there are user permission groups
- Same principles as pre-auth port ACL
- TCAM restrictions apply!

Downloadable ACL List > **PERMIT_ALL_TRAFFIC**

Downloadable ACL

* Name	PERMIT_ALL_TRAFFIC
Description	Allow all Traffic
* DACL Content	permit ip any any

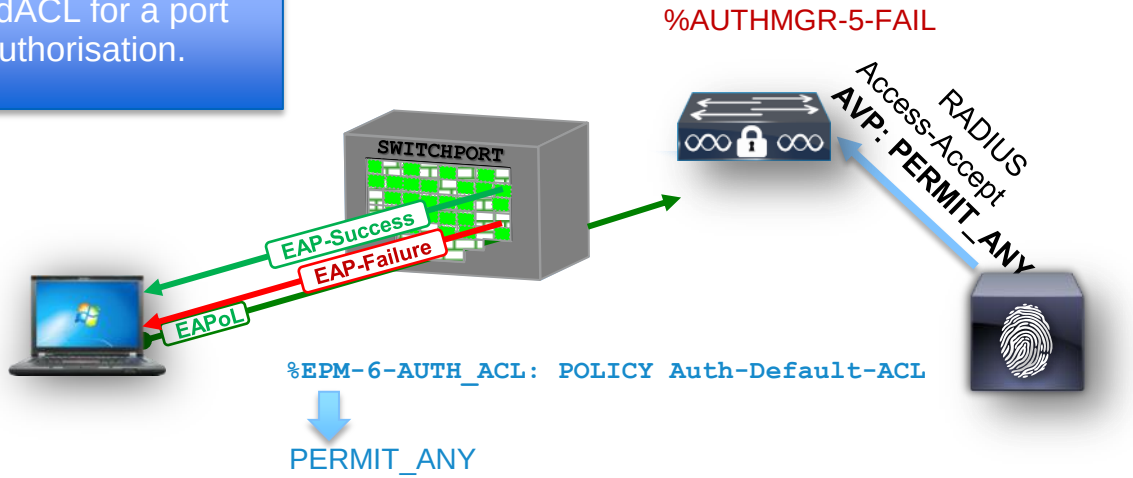
ACL Rules of Thumb

- Whenever possible, use downloadable ACLs
  - Wired environments
  - Wired / Wireless environments with Catalyst 3850 / 5760 (Unified Access)
  - Wired / Wireless environments (traditional) use dACLs for wired and Filter-id for the wireless part
- When dACLs are not possible (no ACS / ISE)
  - Distributed Deployments: use Filter-id ACLs
  - Centralised Deployments: use per-user ACLs

Handling dACLs without PACLs

Before 12.2(54)SG and 12.2(55)SE

A switch that receives a dACL for a port without a PACL will fail authorisation.



After 12.2(54)SG and 12.2(55)SE

The switch will automatically attach a default PACL called “Auth-Default-ACL” and then apply dACL.

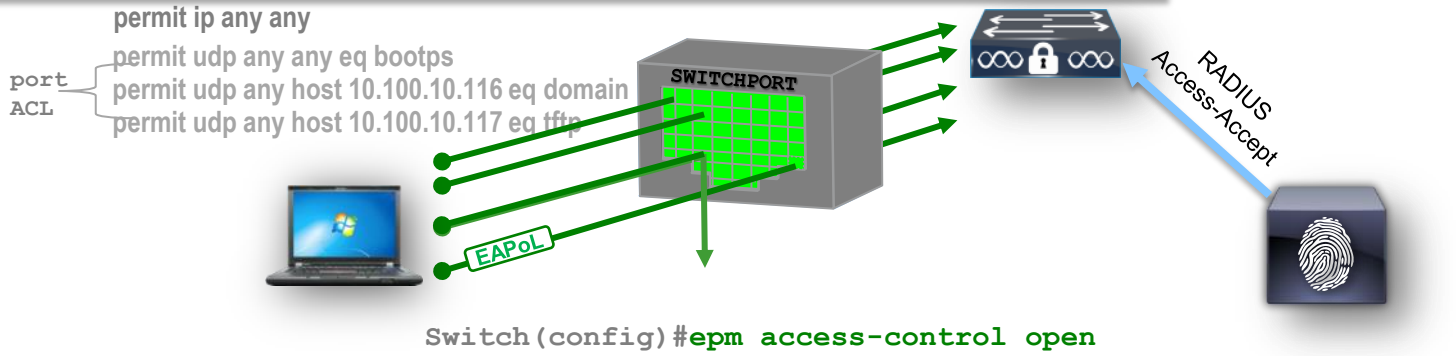
Tip: Use For Graceful Transition from Monitor Mode

Reduce Dynamic ACL Configuration

Default behaviour:

If no dynamic ACL is downloaded, Pre-Auth Port ACL controls the port.

Every endpoint must be assigned a dynamic ACL.




```
Switch(config)#epm access-control open
```

With “open directive” configured:

If the RADIUS server returns a dynamic ACL, dynamic ACL is applied.

If no dynamic ACL returned, switch automatically creates a “permit” entry for the authenticated host.

12.2(54)SG
12.2(55)SE

Low Impact In a Nutshell

Summary

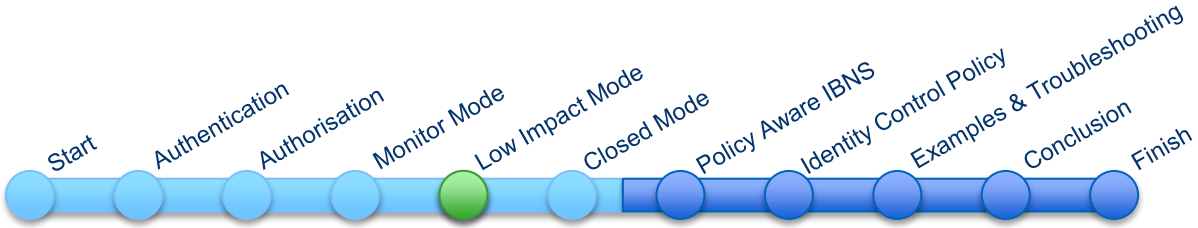
- Default open + pre-auth ACL
- Differentiated access control using dynamic IPv4 ACLs

Benefits & Limitations

- Minimal Impact to Endpoints
- Minimal Impact to Network
- No L2 Isolation
- Some access prior to authentication

Recommendations

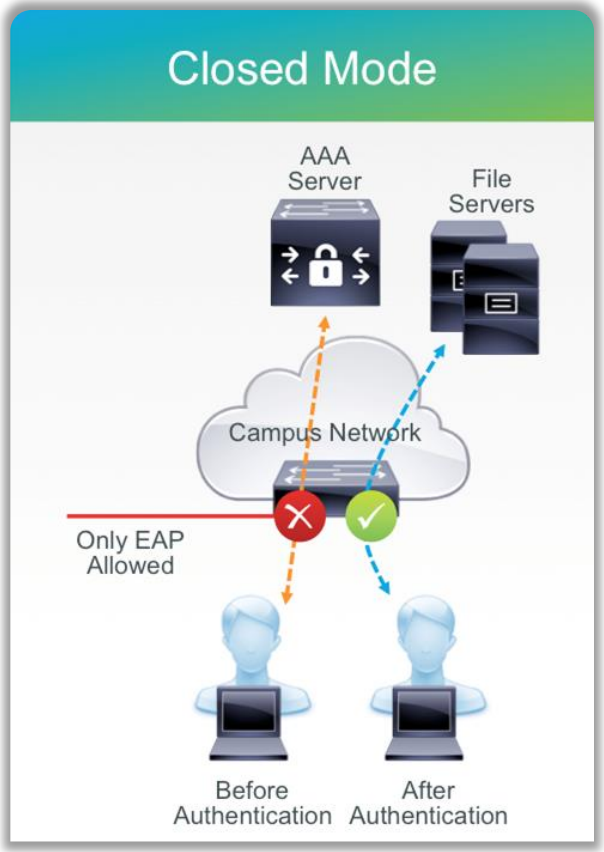
- Start with least restrictive port ACLs
- Use downloadable ACLs if you have ACS / ISE
- Use ‘Open’ Directive to reduce dACL config






Implementing Phased Deployments
‘Closed Mode’

Scenario 3: Closed Mode



Closed Mode Goals

- No access before authentication
- Rapid access for non-802.1X-capable corporate assets
- Logical isolation of traffic at the access edge

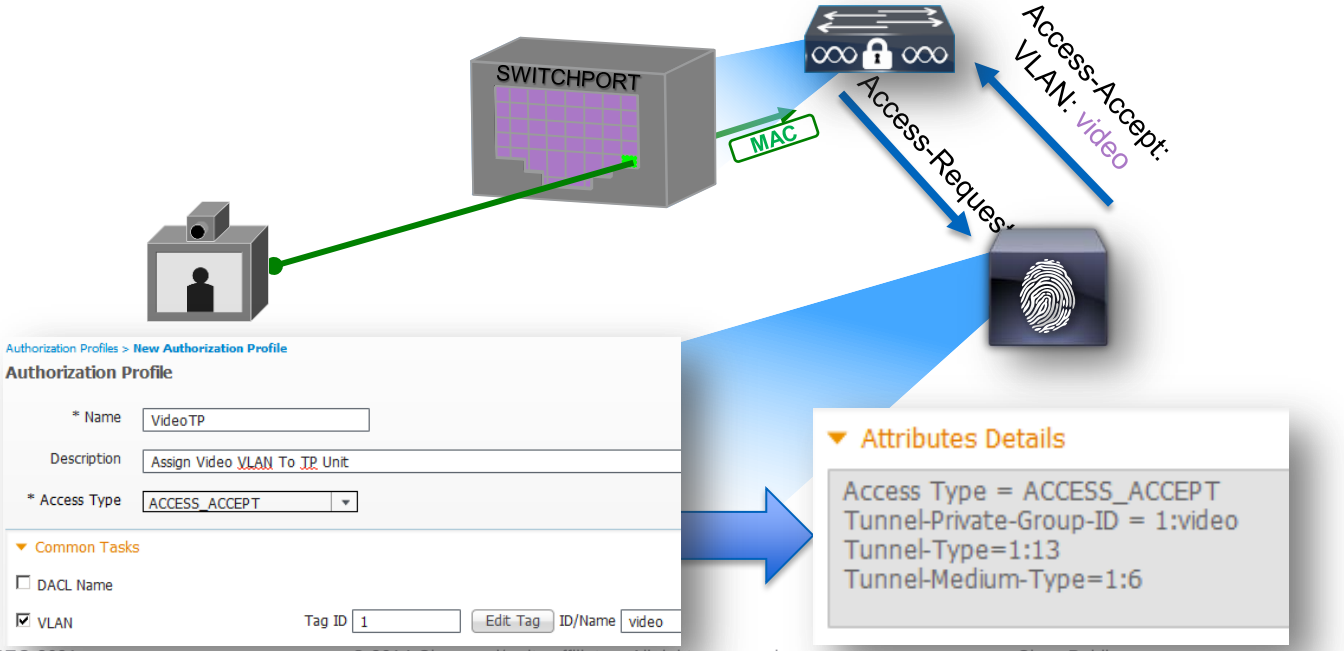
Network Virtualisation Solution
See BRKCRS-2033 for more on Network Virtualisation

Closed Mode: How To

- Return to default “closed” access
- Timers or authentication order change
- Implement identity-based VLAN assignment

Closed Mode: AAA Server

- If no VLAN sent, switch will use static switchport VLAN
- Configure dynamic VLANs for any user that should be in different VLAN



Dynamic VLANs Impact Your Network

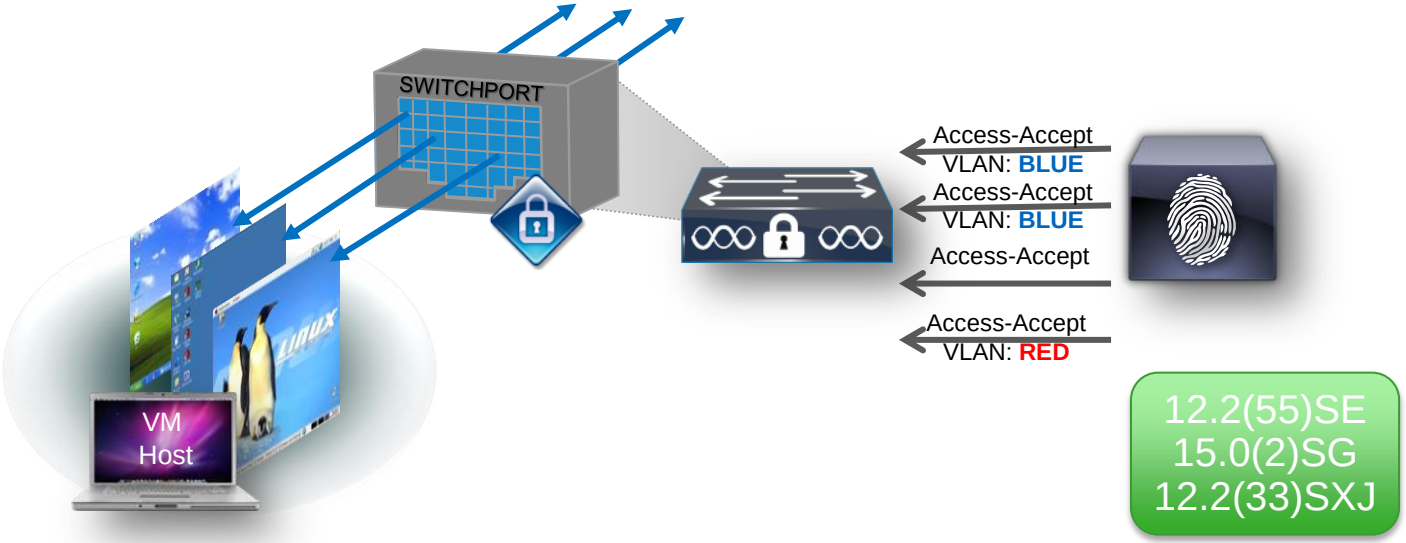
- More VLANs To Trunk (Multi-Layer Deployments)
- More Subnets to Route
- Every Assignable VLAN Must Be Defined on Every Access Switch
- More DHCP Scopes (and addresses) to manage

Network	Interface
10.10.10.x/24	Gi0/1
10.10.20.x/24 10.10.30.x/24	Gi0/2 Gi0/3
10.10.40.x/24	Gi0/4
10.10.50.x/24	Gi0/5

VLAN 10: DATA	10.10.10.x/24
VLAN 20: VOICE	10.10.20.x/24
VLAN 30: MACHINE	10.10.30.x/24
VLAN 40: ENG	10.10.40.x/24
VLAN 50: UNAUTH	10.10.50.x/24

Best Practice: Use the Fewest Possible Number of VLANs

Limited Dynamic VLAN Assignment with Multi-Auth



- First successful authentication “locks” the Data VLAN
- Subsequent endpoints must get assigned same VLAN or no VLAN
- Blue VLAN=Permit, No VLAN=Permit, Red VLAN=Deny (Local)

Catalyst 3850 & 3650: Per-Session VLAN Assignment

"MAC based VLANs"

- Before Cat3850 / Cat3650: One port, one VLAN per access port (1:1)
- Exception: Voice (one Data Device untagged, one Voice Device tagged w/ VVLAN)
- Later: Allowing VLAN assignment on multi-authentication ports, but first device 'rules' the port.
- **Now with Catalyst 3850 & 3650: Each session can have individual VLAN assigned**

160	WIRED-EMPLOYEE	active	Gi1/0/13
170	WIRED-GUEST	active	Gi1/0/13

Extending the Network Edge

12.2(33)SXJ

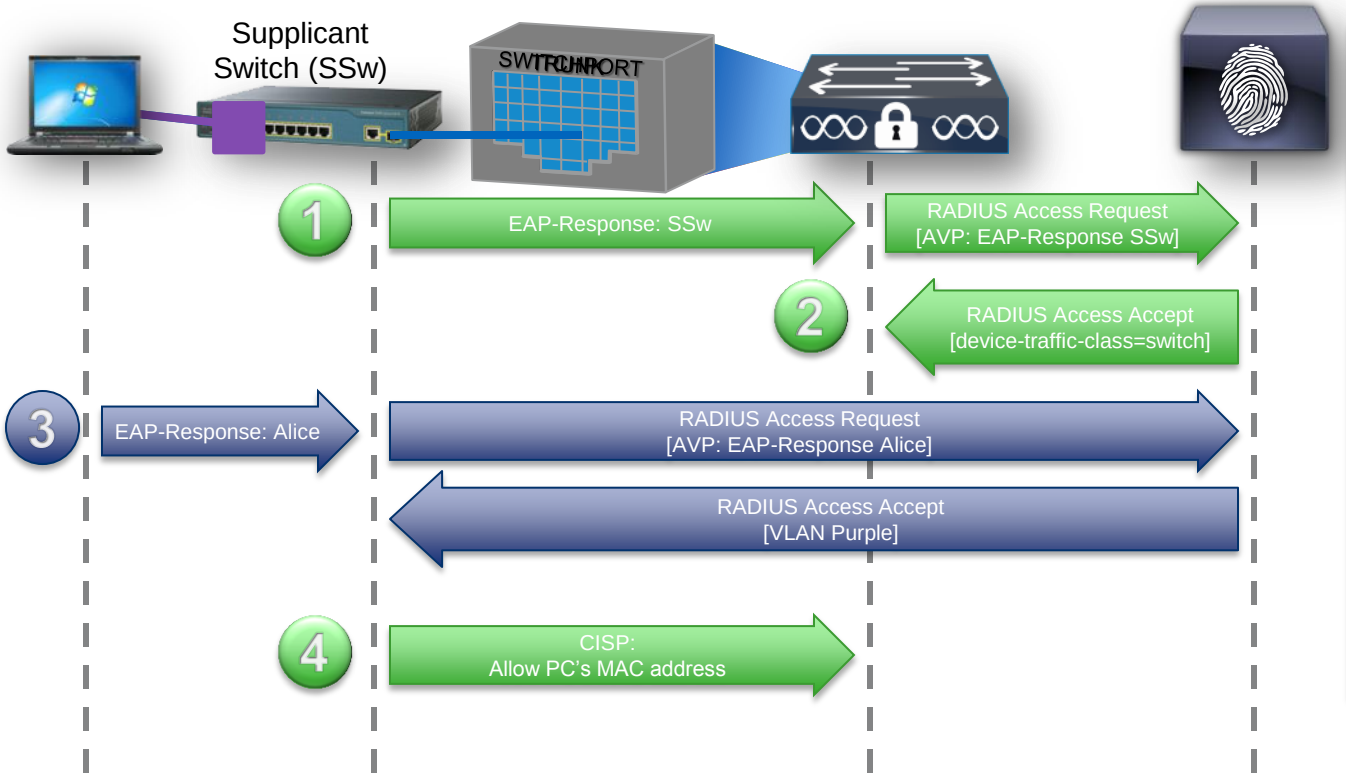
Hubs on an 802.1X network:

- introduce multiple MACs per port
- may not actually be hubs
- are not managed devices

Ideally, *extended edge*:

- Extends trust and policy
- Uses a managed device
- Works on any access port

Network Edge Authentication Topology (NEAT)



1. NEAT-capable SSw authenticates itself to Authenticator Switch (ASw)
2. ASw converts port to trunk
3. SSw authenticates users and devices in conference room
4. ASw learns authenticated MACs via CISP

CISP = Client Information Signalling Protocol

NEAT Configuration Example

Supported Supplicant EAP Methods

- EAP-FAST
- EAP-GTC
- EAP-LEAP
- **EAP-MD5**
- EAP-MSCHAPV2
- EAP-PEAP
- EAP-TLS

SSw

Global Config

```
cisp enable
dot1x supplicant controlled transient
dot1x supplicant force-multicast
dot1x credentials DOT1X-NEAT
  username 2960-8PC-static
  password 0 geheim
!
eap profile EAP-NEAT
  method md5
!
interface GigabitEthernet1/0/1
 description Connected to ASw
 switchport trunk encap dot1q
 switchport mode trunk
 dot1x pae supplicant
 dot1x credentials DOT1X-NEAT
 dot1x supplicant eap profile EAP-NEAT
!
```

Network Access Users

Edit | Add | Change Status | Import | Export

Status	Name	Description	First
Enabled	2960-8PC-s...	2960 Compact Switch	

ASw

Global Config

```
cisp enable
!
interface GigabitEthernet5/1
 description connected to SSw
 switchport access vlan 100
 switchport mode access
 dot1x pae authenticator
 authentication port-control auto
!
```

AutoConfig Apply Macro

```
no spanning-tree bpduguard enable
no switchport access vlan 100
no switchport nonegotiate
switchport trunk native vlan 100
spanning-tree portfast trunk
switchport mode trunk
```

Cisco:cisco-av-pair = device-traffic-class=switch

Attributes Details

Access Type = ACCESS_ACCEPT
cisco-av-pair = device-traffic-class=switch

Closed Mode In a Nutshell

Summary

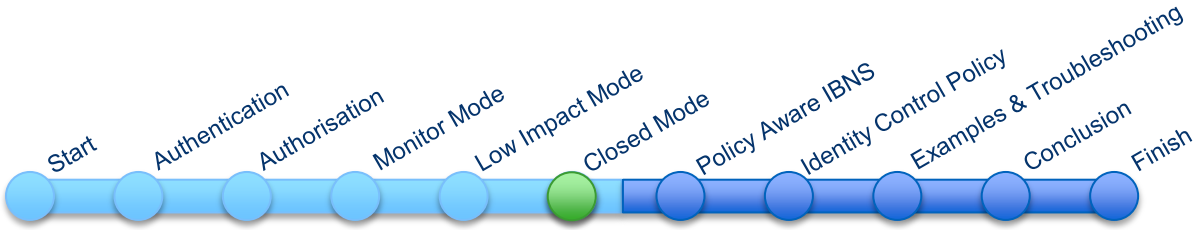
- Default closed
- Differentiated access control using dynamic VLANs

Benefits & Limitations

- Logical Isolation at L2
- No Access for Unauthorised Endpoints
- Impact to Network
- Impact to Endpoints

Recommendations

- Use fewest VLANs possible
- Know which devices can't change VLANs
- User Distribution helps with VLAN names
- Enable Critical Voice VLAN
- Consider NEAT as needed

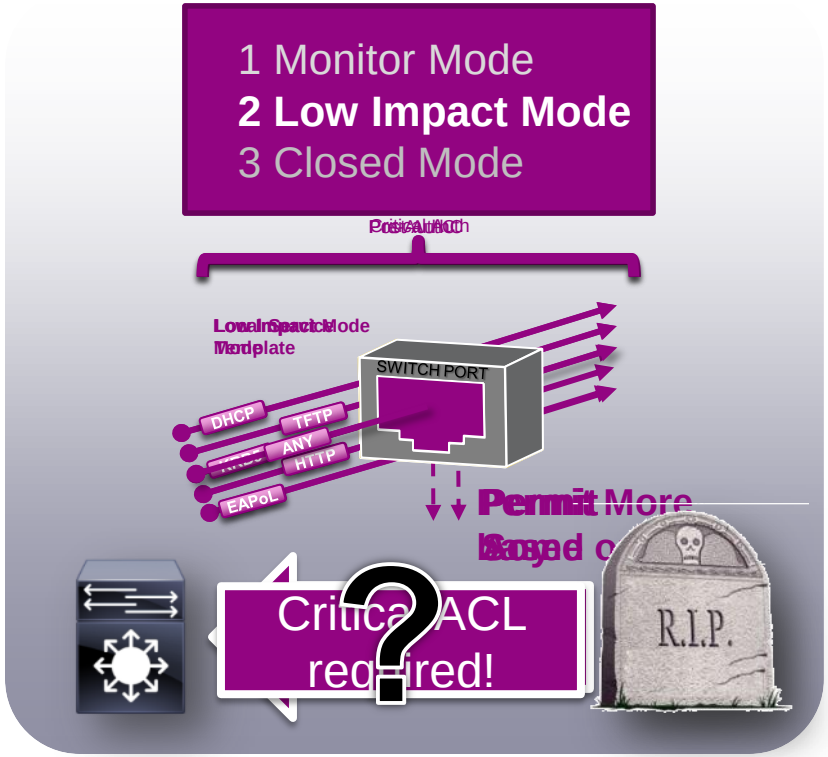





IOS Identity Evolution: Policy Aware IBNS

Evolving Deployment Scenarios

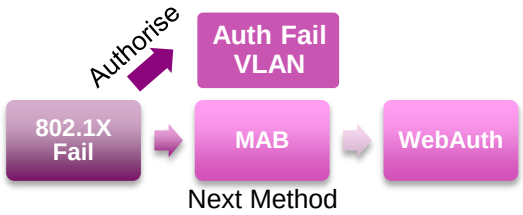
- Popular Deployment Scenarios
  - Demonstrating Industry Leadership
  - Phased Deployments → Clear Plan of Action
  - High Visibility + Incremental Access Control
- Now You Want More!
  - “What if AAA goes down?”
  - What about IPv6 ACLs?
- The Need for Flexible Authorisation
  - ACL, VLAN, QoS, URL-Redirect, IPv6 enabled identity…
  - Flex Authentication **plus** Flex Authorisation



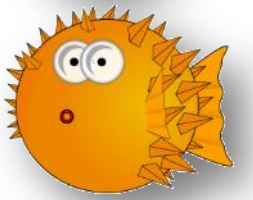
Challenges with Current Model

A few Examples…

- **Flex Auth:** Hard Coded Rules, Timing / Order dependency, no concurrent authentication
- **WebAuth:** Auth in Access VLAN, no IPv6 support, Authorisation by ACL only
- **IPv6:** Device Tracking, URL Redirect, IPv6 dACL, Guest Access, Local WebAuth
- **Configuration:** dynamic changes with NEAT / ASP, Configuration size



Wanted: First Class Web Auth



Introducing*: Policy-Aware IBNS

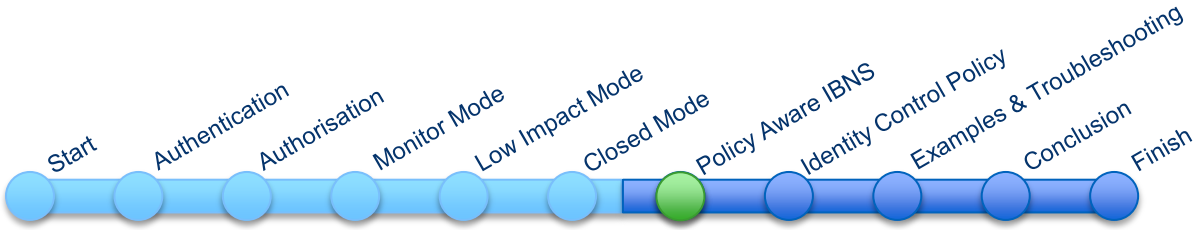
In a Nutshell

New Identity Policy Engine (Access Policy)

ANY Authentication Method with ANY Authorisation Feature on ANY Media

Leverages Templates for Sessions and Interfaces

*Available on Catalyst 3650/3850 at FCS on 2k/3k/4k with 15.2(1)E/3.5.0E and on 6k with MK2 1HCY14






Policy Aware Identity

Identity Control Policy

Your Every Day Policy Management

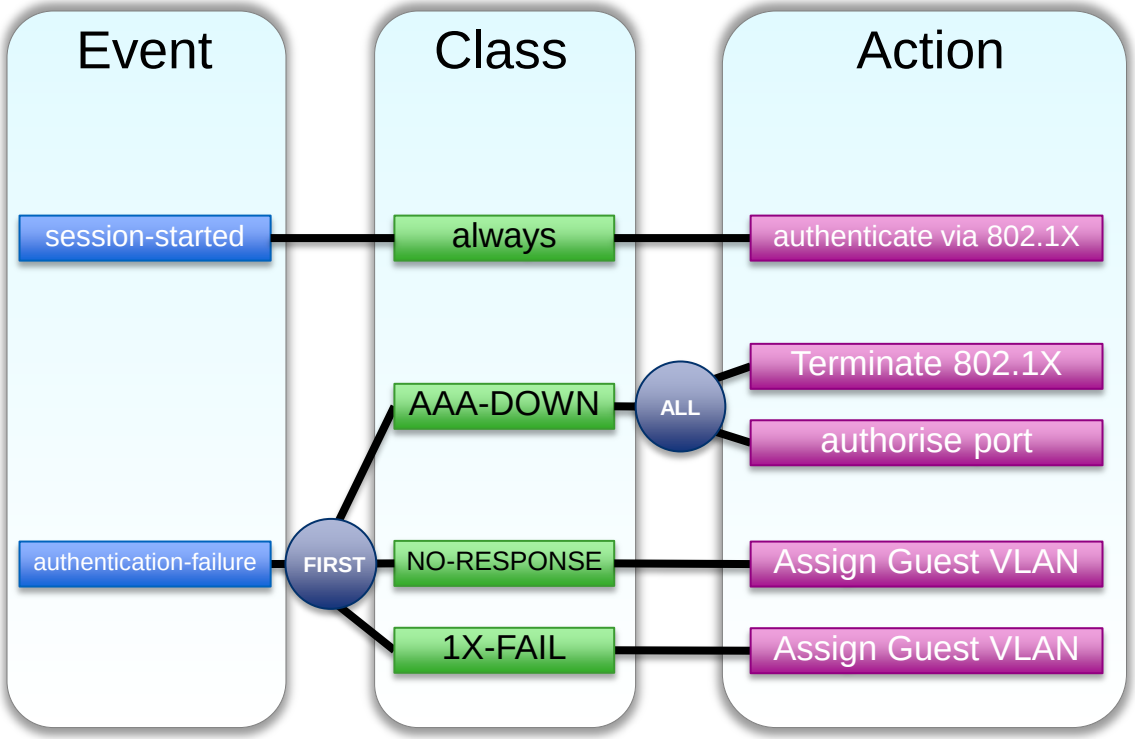
What's an Event? What's a Class? What's an Action?

E-Mail Policy (aka Inbox Filtering)

- **Event:** E-Mail arrives
- **Class:** additional Attributes
  - Sender is Wife
  - Mail is Spam
  - Mail is addressed to Mail List
- **Action:** Result, based on Class
  - Wife: 1) Mark Urgent 2) Put in Inbox
  - Spam: 1) Mark as Spam 2) Delete
  - Marketing 1) Put in Marketing Folder

From E-Mail Policy to Identity Control Policy

The Concept still Applies...

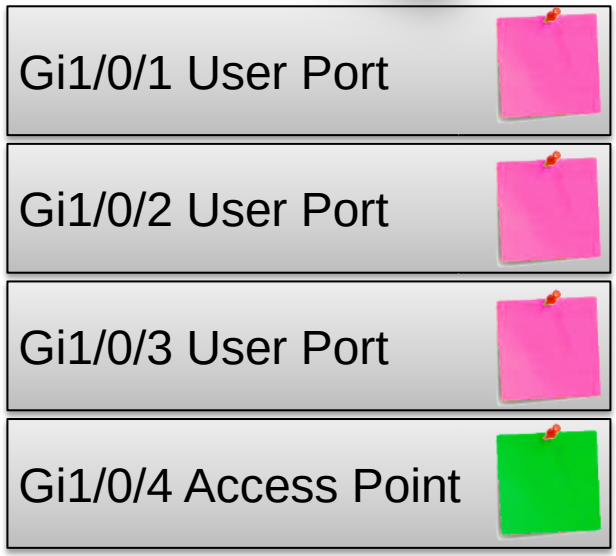


Templates

Dynamic Configuration Done the Right Way

Configuration by Reference:

- Service Templates
  - will be dynamically assigned to a session
  - can be locally defined -or-
  - downloaded via RADIUS
- Interface Templates**
  - Cure for the Configuration Bloat
  - Generic tool, not restricted to Session / Identity
  - Like Port Profiles on NX-OS



**Will be available in a future release

Service Template Example

Using a Critical Auth Example

```
service-template CRITICAL
   description allow all traffic
   access-group PERMIT-IPV4-ANY
   access-group PERMIT-IPV6-ANY
!
```

Example and Available Commands

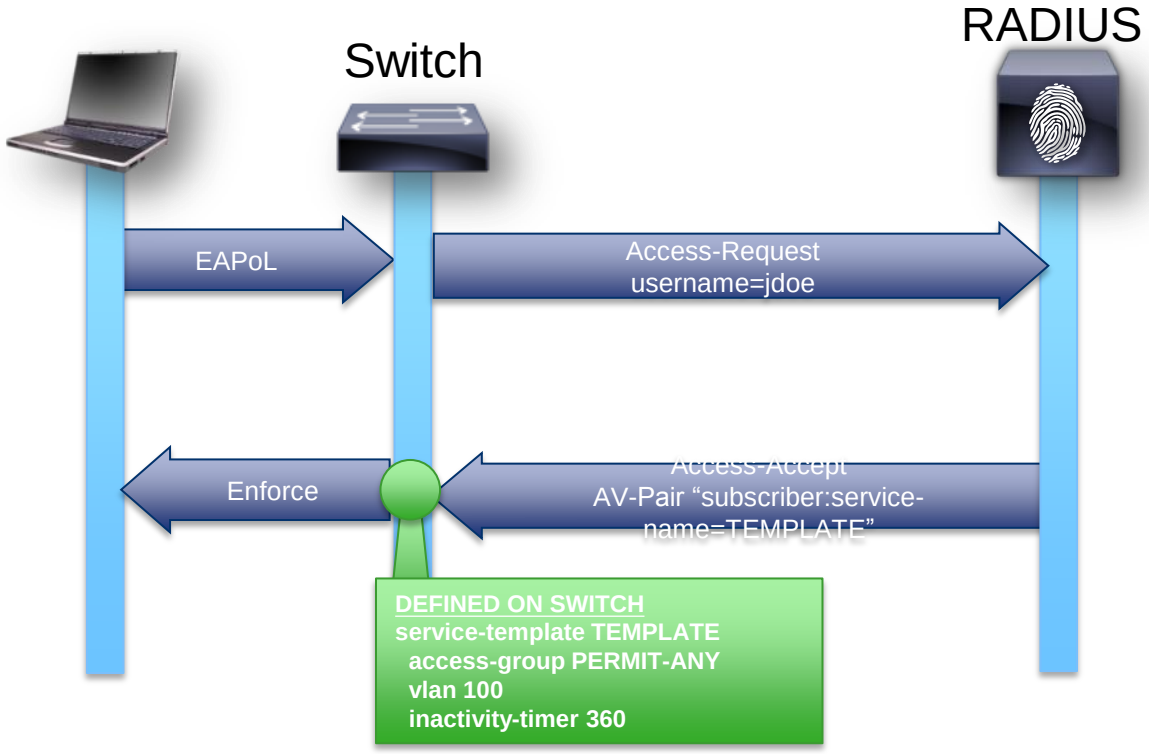
```
switch(config)#service-template CRITICAL
switch(config-service-template)#?
service-template configuration commands:
  absolute-timer     Absolute timeout value in seconds
  access-group       Access list to be applied
  description        Enter a description
  exit               Exit identity policy configuration submode
  inactivity-timer   Inactivity timeout value in seconds
  no                 Negate a command or set its defaults
  redirect           Redirect clients to a particular location
  tag                tag name
  tunnel             tunnel for wired client access
  vlan               Vlan to be applied
  voice              Voice feature

switch(config-service-template)#
```

- Can be defined locally on the switch
- Can also be defined on the RADIUS server and downloaded dynamically as needed per authorisation or during CoA (ISE 1.2 Feature)
- Used as one of the Actions per Control-Policy or as part of the RADIUS Authorisation (AV Pair)
- Templates via AAA can contain arbitrary AV Pairs

Applying a Template

Similar to Applying a Port ACL via *filter-id*



- Can also be triggered via RADIUS CoA
- Service-Templates activation can be a local Control Policy action
- If it doesn't exist, it can be downloaded like an dACL

Service Template Download from AAA

TEMPLATES RADIUS-Cisco:cisco-av-pair equals download-request=service-template SVC_TEMPLATES

Access Policies > Access Services > SVC_TEMPLATES > Identity

Single result selection Rule based result selection

Identity Source: Internal Users Select

Advanced Options

If authentication failed Continue

If user not found Continue

If process failed Drop

ACS

Authorization Profiles > New Authorization Profile

Authorization Profile

* Name TL-USER

Description Service Template For Users

* Access Type ACCESS_ACCEPT

Service Template ☑

ISE

ACS / any RADIUS Server

- Incoming request tagged with *cisco-av-pair="download-request=service-template"*
- Template-Name = Username
- Trivially Pass Authentication (username is the template name)
- Template Content is defined by AV pairs returned in authorisation rules

ISE 1.2 and newer

- Template support is built-in

Putting the Pieces Together

Policy Configuration Elements

```
aaa […]
radius […]
dot1x system-auth-control

ip access-list […]
ipv6 access-list […]

service-template […]
service-template […]

class-map […]
class-map […]
policy-map […]

interface range gi1/0/1 – 48
  mab
  access-session port-control […]
  service-policy type control subscriber […]
```

- Global Configuration (AAA,802.1X, CoA, ACLs, etc.)
- Template Configuration (optional)
- Global Policy Configuration (policy-map referencing class-maps)
- Per-Interface Configuration
- References to other Policy Elements (static or dynamic)

Legacy Configuration to New-style Mode

Typical Identity Configuration (today)

```
interface GigabitEthernet1/0/1
 switchport access vlan 100
 switchport mode access
 ip access-group IPV4-PRE-AUTH-ACL in
 authentication control-direction in
 authentication event fail action authorize vlan 100
 authentication event server dead action authorize vlan 100
 authentication event no-response action authorize vlan 100
 authentication open
 authentication order dot1x mab
 authentication priority dot1x mab
 authentication port-control auto
 authentication periodic
 authentication timer reauthenticate server
 authentication timer inactivity server dynamic
 authentication violation restrict
 mab
 dot1x pae authenticator
 dot1x timeout tx-period 5
 spanning-tree portfast
```

switch# authentication display new-style

New Policy mode

```
interface GigabitEthernet1/0/1
 ....
 access-session port-control auto
 access-session host-mode single-host
 service-policy type control subscriber POLICY_Gi1/0/1
 ....
!
policy-map type control subscriber POLICY_Gi1/0/1
 event session-started match-all
  10 class always do-until-failure
   10 authenticate using dot1x retries 2 retry-time 0 priority 10
....
!
class-map type control subscriber match-all DOT1X
 match method dot1x
class-map type control subscriber match-all MAB
 match method mab
....
```

Configuration Mode Display

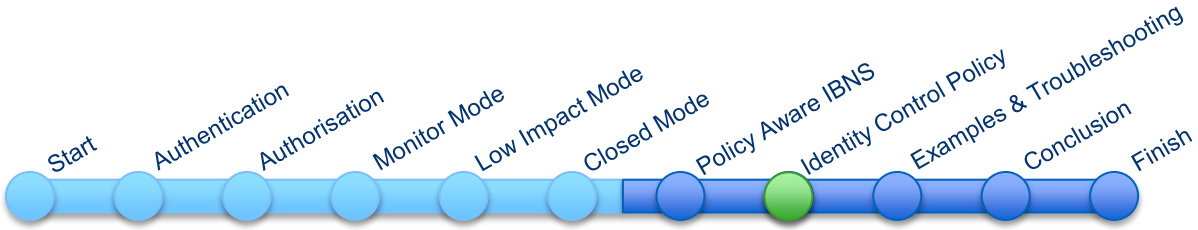
Bridging the Gap Between 'Old World' and 'New World'

Tip: Start with known good configuration and see how changes in 'legacy mode' change the new configuration!

- Existing configurations 'simply work'
- Converting in the background to new Policy Mode
- Use CLI to change how configuration is shown:

```
– switch# authentication display ?
–   legacy      Legacy configuration
–   new-style   New style (c3pl) configuration
```

- If Policy Mode configuration is changed or rebooted in Policy Mode, the change is non-reversible
- No IPv6 capable WebAuth in Old Style Mode
- **This is transient and 'Exec mode' only (does not appear in configuration).**

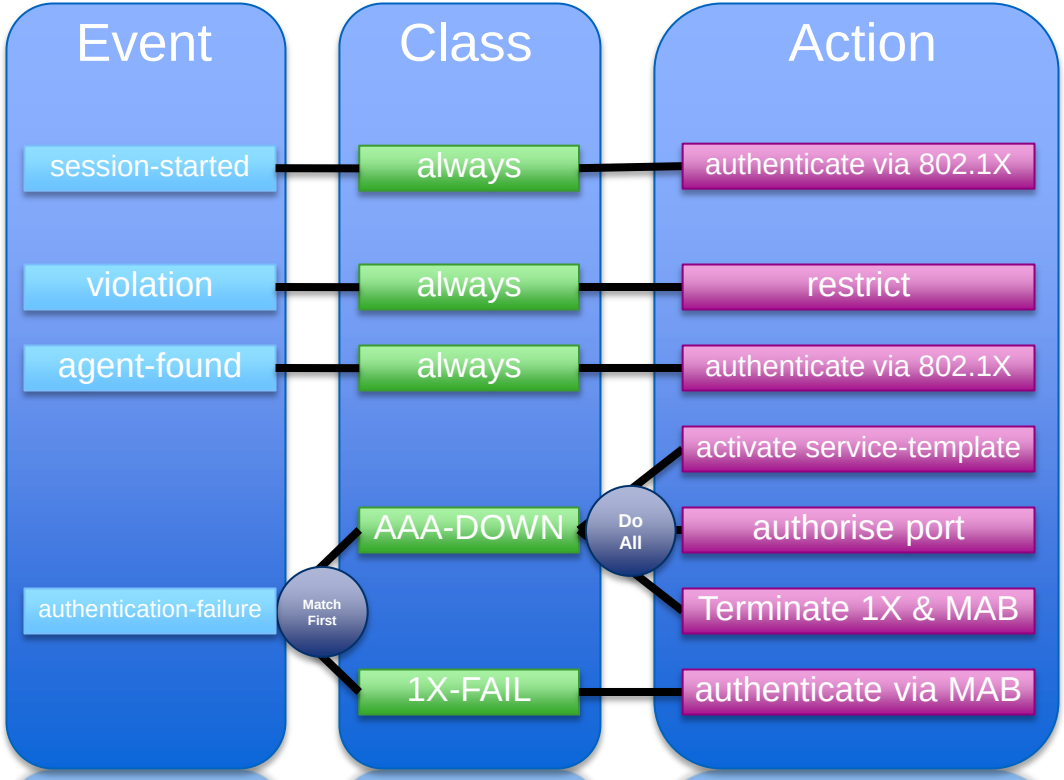





Policy Aware Identity
Examples & Troubleshooting

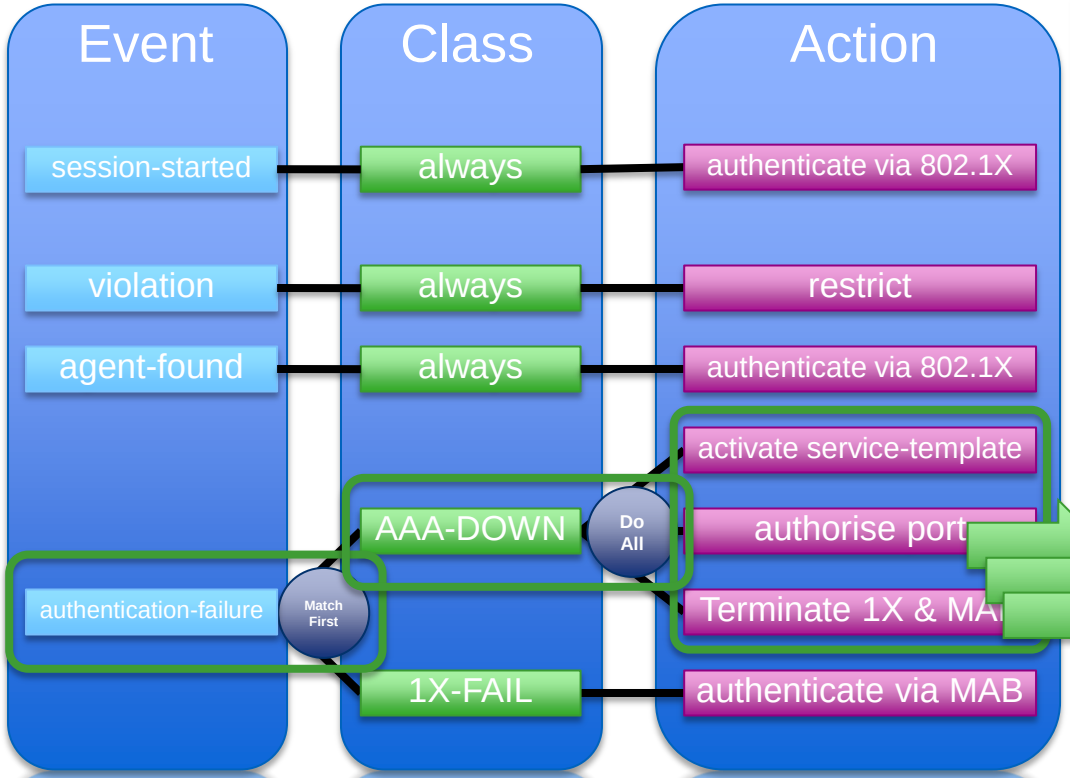
Critical ACL

Configuration Example



Critical ACL

Configuration Example




```
service-template CRITICAL
 access-group CRITICAL-V4
 access-group CRITICAL-V6
!
!
policy-map type control subscriber DOT1X
 event session-started match-all
  10 class always do-until-failure
   10 authenticate using dot1x
 event violation match-all
  10 class always do-all
   10 restrict
 event agent-found match-all
  10 class always do-all
   10 authenticate using dot1x
 event authentication-failure match-first
  10 class AAA-DOWN do-all
   10 activate service-template CRITICAL
   20 authorize
   30 terminate dot1x
   40 terminate mab
  20 class 1X-FAIL do-all
   10 authenticate using mab
```

Additional Examples

Concurrent Authentication

- Pro: Faster Onboarding
- Con: More auths per sec

```
event session-started match-all
  10 class always do-until-failure
   10 authenticate using dot1x priority 10
   20 authenticate using mab priority 20
```

Differentiated Authentication

- Fallback to different user DB based on policy
- No single dot1x ID store anymore!

```
event authentication-failure match-first
 10 class AAA_SVR_DOWN_UNAUTHD_HOST do-↲
         until-failure
  10 terminate mab
  20 terminate dot1x
  30 authenticate using mab aaa authc-↲
     list mab-local authz-list mab-local
```

IPv6 Device Discovery

- Enable IPv6 Device Tracking
- Make Identity Policy IPv6 aware
- Note: Define which VLANs to apply and also trust the uplink port

```
!
ipv6 snooping policy v6-snoop
 trusted-port
!
vlan configuration 100-180
 ipv6 nd suppress
 ipv6 snooping
!
interface TenGig1/1/1
 description *** uplink ***
 [ ... ]
 ipv6 snooping attach-policy v6-snoop
!
```

Troubleshooting Control Policy

New Session Display

Old Friends with new Names:

```
switch#sh access-session int gi1/0/13 detail
            Interface:  GigabitEthernet1/0/13
               IIF-ID:  0x103B240000000D9
          MAC Address:  0800.27f0.7969
         IPv6 Address:  FE80::A00:27FF:FEF0:7969,
2001:DB8:1:170:C025:2462:AF2A:477B
         IPv4 Address:  172.16.30.66
            User-Name:  harips@ibns.lab
               Status:  Authorized
               Domain:  DATA
       Oper host mode:  multi-auth
     Oper control dir:  both
      Session timeout:  N/A
    Common Session ID:  AC101D020000115B11DEEC8C
      Acct Session ID:  0x0000122B
               Handle:  0xD8000001
       Current Policy:  POLICY_Gi1/0/13

Server Policies:
              ACS ACL:  xACSACLx-IP-permit-most-50b5f56e
        Template: EMPLOYEE_1 (priority 100)
           Vlan Group:  Vlan: 160
              ACS ACL:  xACSACLx-IP-permit-most-50b5f56e

Method status list:

       Method           State
       dot1x            Authc Success
       mab              Stopped
```

'show access-session' instead of 'show authentication session'

IPv6 awareness

Applied Policies (here: with server assigned Template)

Troubleshooting Control Policy

(cont.)

And new Friends:

```
newton-1#sh policy-map type control subscriber name
POLICY_Gi1/0/13
Control_Policy: POLICY_Gi1/0/13
  Event:       event session-started match-all
    Class-map:  10 class always do-until-failure
      Action: 10 authenticate using dot1x retries 2 […]
      Executed: 2

  Event:       event authentication-failure match-first
    Class-map:  10 class DOT1X_NO_RESP do-until-failure
      Action: 10 terminate dot1x
      Executed: 43

      Action: 20 authenticate using mab priority 20
      Executed: 43

    Class-map:  20 class MAB_FAILED do-until-failure
      Action: 10 terminate mab
      Executed: 0

      Action: 20 authentication-restart 60
      Executed: 0
[…]
```

'show policy-map type control' to show the control policy

See complete Policy (Events, Classes, Actions)

Look for specific events and how often associated classes matched and actions have been executed

Troubleshooting Control Policy

(cont.)

- debug pre* all | error | **event** | ha | prr | **rule**
- To understand policy flow and identify events and actions
- Powerful in combination with conditional debugging ('debug condition')

New Event

Evaluated Class-Map & Match!

Associated Action

Single Event

Next Event

```
[PRE:RULE:EVENT:D8000001] Executing policy-map type control subscriber POLICY_Gi1/0/13
[PRE:RULE:EVENT:D8000001]   event session-started match-all
[PRE:RULE:EVENT:D8000001]     class always do-until-failure policy instance 0x5A000038
[PRE:RULE:EVENT:D8000001] Evaluate: class-map type control match-all subscriber always
[PRE:RULE:EVENT:D8000001] evaluated class map: success
[PRE:RULE:EVENT:D8000001] Executing 'dot1x' for client (0800.27f0.7969) on Interface Gi1/0/13 AuditSessionID AC101D020C
[PRE:RULE:EVENT:D8000001] Action authenticate using dot1x retries 2 retry-time 0 priority 10:sync:success
[PRE:RULE:EVENT:D8000001] executed action handlers and returning with status:1, result:0

[PRE:RULE:EVENT:D8000001] Executing policy-map type control subscriber POLICY_Gi1/0/13
[PRE:RULE:EVENT:D8000001]   event agent-found match-all
[PRE:RULE:EVENT:D8000001]     class always do-until-failure policy instance 0x5A000038
[PRE:RULE:EVENT:D8000001] Evaluate: class-map type control match-all subscriber always
[PRE:RULE:EVENT:D8000001] evaluated class map: success
[PRE:RULE:EVENT:D8000001] Action terminate mab:sync:success
[PRE:RULE:EVENT:D8000001] Action authenticate using dot1x retries 2 retry-time 0 priority 10:sync:success
[PRE:RULE:EVENT:D8000001] executed action handlers and returning with status:1, result:0
%DOT1X-5-FAIL: Authentication failed for client (0800.27f0.7969) on Interface Gi1/0/13 AuditSessionID AC101D0C
switch#
```

*PRE = Policy Rule Engine

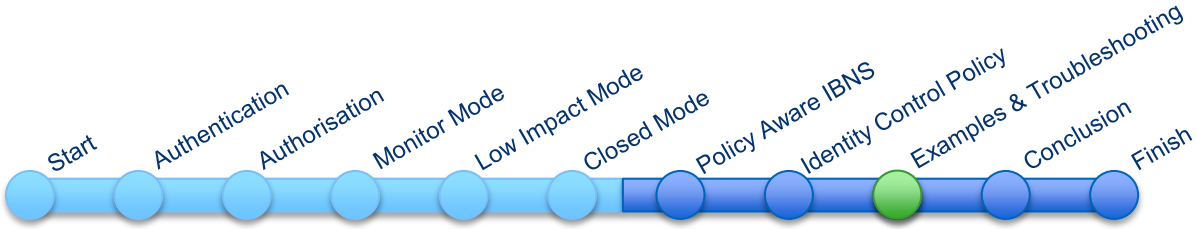
Control Log Verbosity

Suppress ‘Success’ log messages, only log failure

- `no authentication logging verbose`
- `no mab logging verbose`
- `no dot1x logging verbose`
- Default is ‘verbose’!
- Some ISE troubleshooting tools depends on seeing these messages

Selectively Debug

- `debug interface Gi1/0/1`
- Limits effect of debug to given interface


Start
Authentication
Authorisation
Monitor Mode
Low Impact Mode
Closed Mode
Policy Aware IBNS
Identity Control Policy
Examples & Troubleshooting
Conclusion
Finish




Conclusion

Key Takeaways

Start Simple and Evolve

- Monitor mode before access control
- Least restrictive ACLs, fewest VLANs

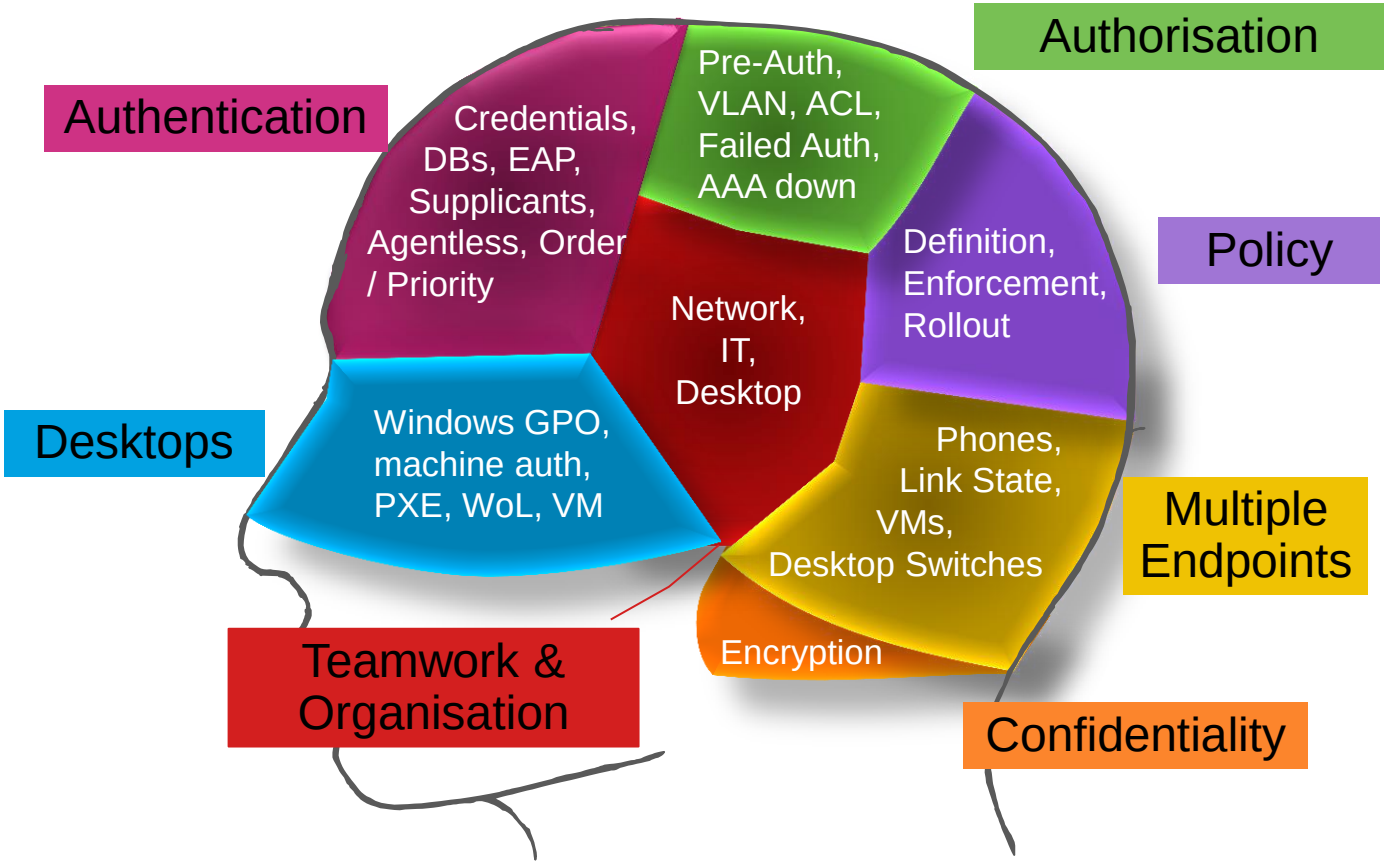
Design / Plan / Implement

- Know where every device & user should / could end up
- For troubleshooting: Start at a central point, work outward as required – a good AAA server is invaluable

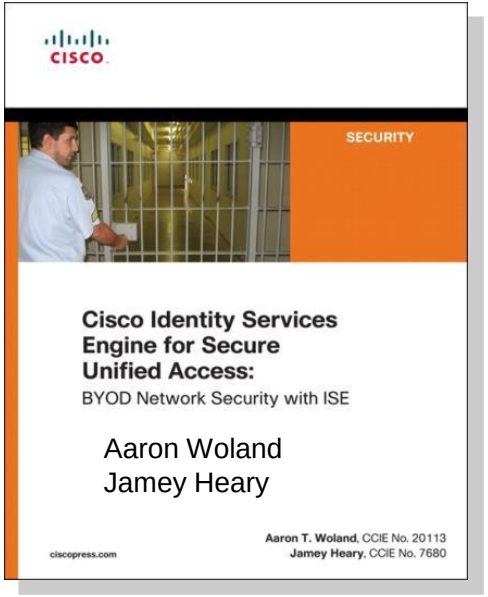
Optimise Deployment Scenarios With New Features

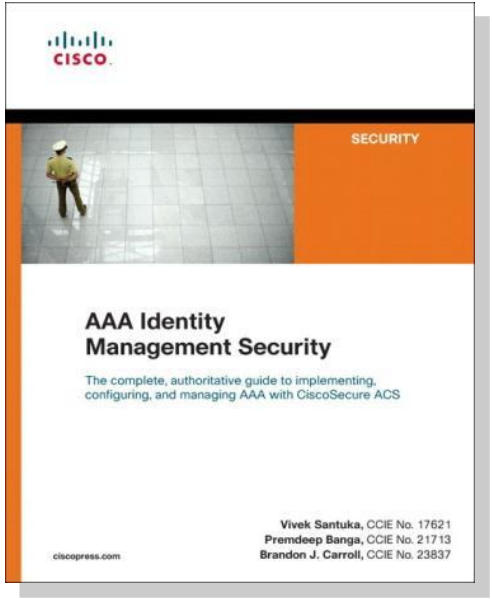
- Adapt new features where available
- Familiarise with new policy model and capabilities

Most Important: Think at the System-Level



Recommended Reading








Q & A

Complete Your Online Session Evaluation

Give us your feedback and receive a Cisco Live 2014 Polo Shirt!

Complete your Overall Event Survey and 5 Session Evaluations.

- Directly from your mobile device on the Cisco Live Mobile App
- By visiting the Cisco Live Mobile Site www.ciscoliveaustralia.com/mobile
- Visit any Cisco Live Internet Station located throughout the venue

Polo Shirts can be collected in the World of Solutions on Friday 21 March 12:00pm - 2:00pm

Learn online with Cisco Live!

Visit us online after the conference for full access to session videos and presentations.
www.CiscoLiveAPAC.com

CISCO™