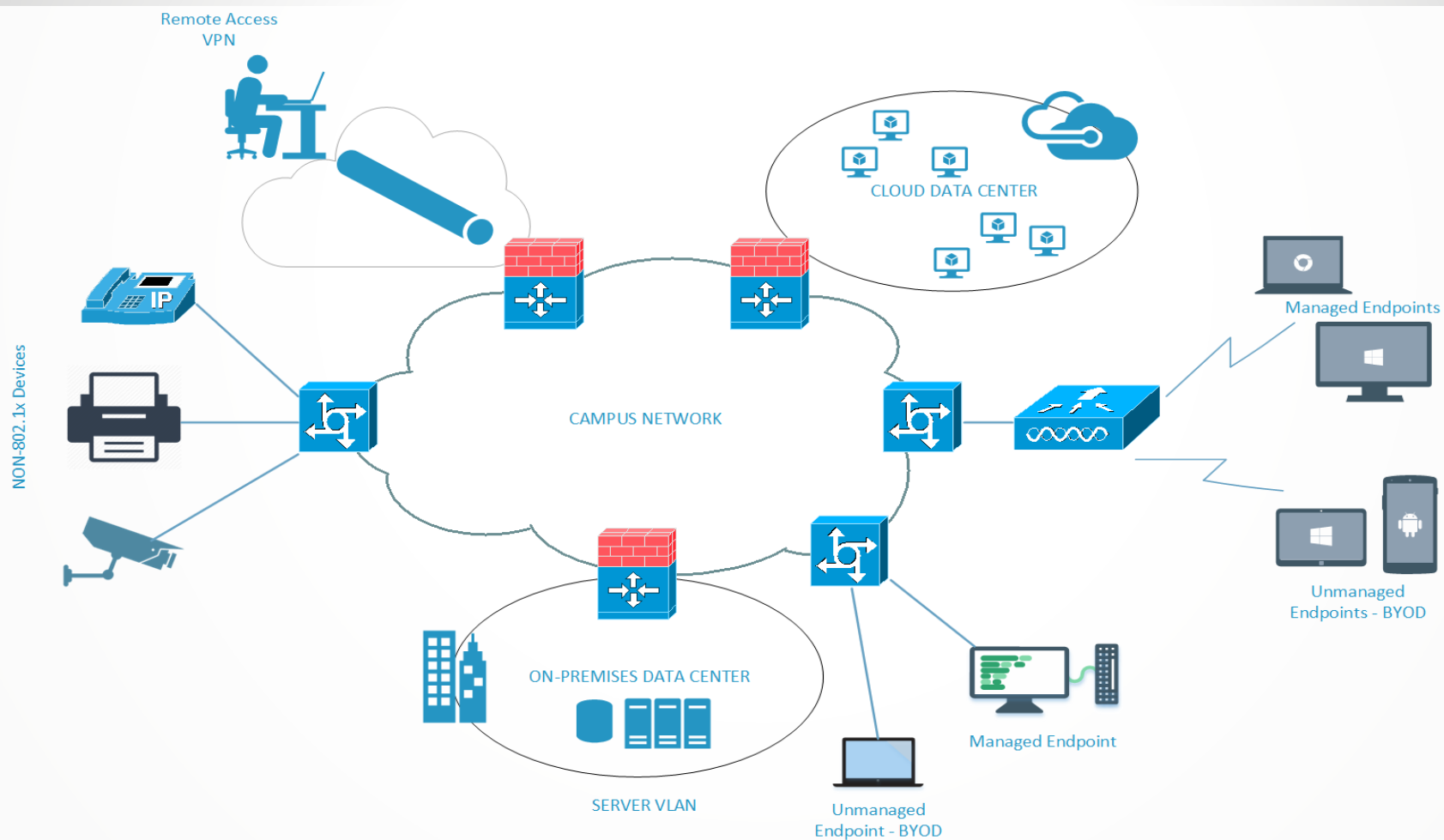


Система контролю доступу до корпоративної мережі на базі Cisco ISE

Жучко Дмитро
Comparex Ukraine

Сучасна мережева архітектура



Основні задачі, що вирішує Cisco ISE



Cisco Identity Services Engine

Керування гостьовим доступом. Організація безпечного доступу гостей до Інтернету та мережевих ресурсів.



BYOD. Визначення політики доступу BYOD пристроїв до корпоративної мережі.



Контроль доступу до мережі в цілому
Визначення політик доступу через дротові, бездротові та VPN мережі.

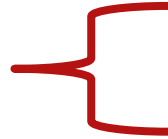


Адміністрування мережевих пристроїв. Керування та організація доступу до мережевих пристроїв використовуючи єдину платформу



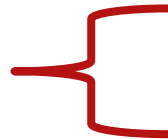
Потреба

Надання повної інформації щодо пристроїв в мережі



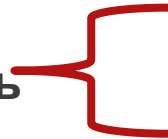
Забезпечення повномасштабного моніторингу пристроїв, що отримують доступ до мережі та їх класифікація досягається вже на першому етапі впровадження – Monitor Mode

Контроль доступу до мережі



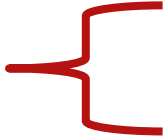
- Забезпечення дотримання політики підключення до дротових та бездротових мереж в масштабах усієї Компанії
- Запобігання несанкціонованого доступу до мережі

Контроль відповідності та ізоляція пристроїв, що не відповідають корпоративним політикам



- Автоматичне ізолювання пристроїв, що не відповідають політикам;
- Виконання операцій, направлених на приведення до відповідності комп'ютерів без залучення адміністратора

Контроль гостьового доступу



- Організація контрольованого доступу гостей до мережі Інтернет (Hotspot Portal)
- Організація безпечного доступу партнерів до інформаційних ресурсів Компанії (Sponsored Portal)

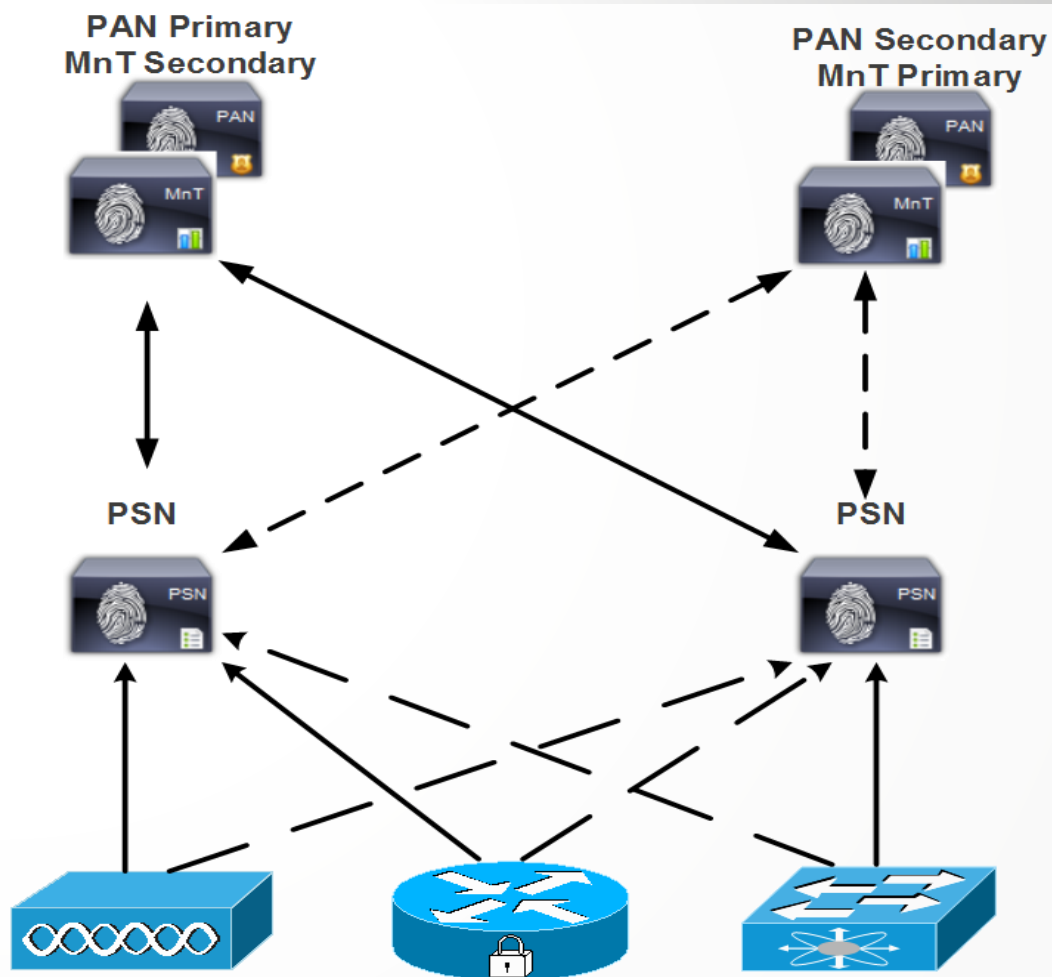
Централізоване керування



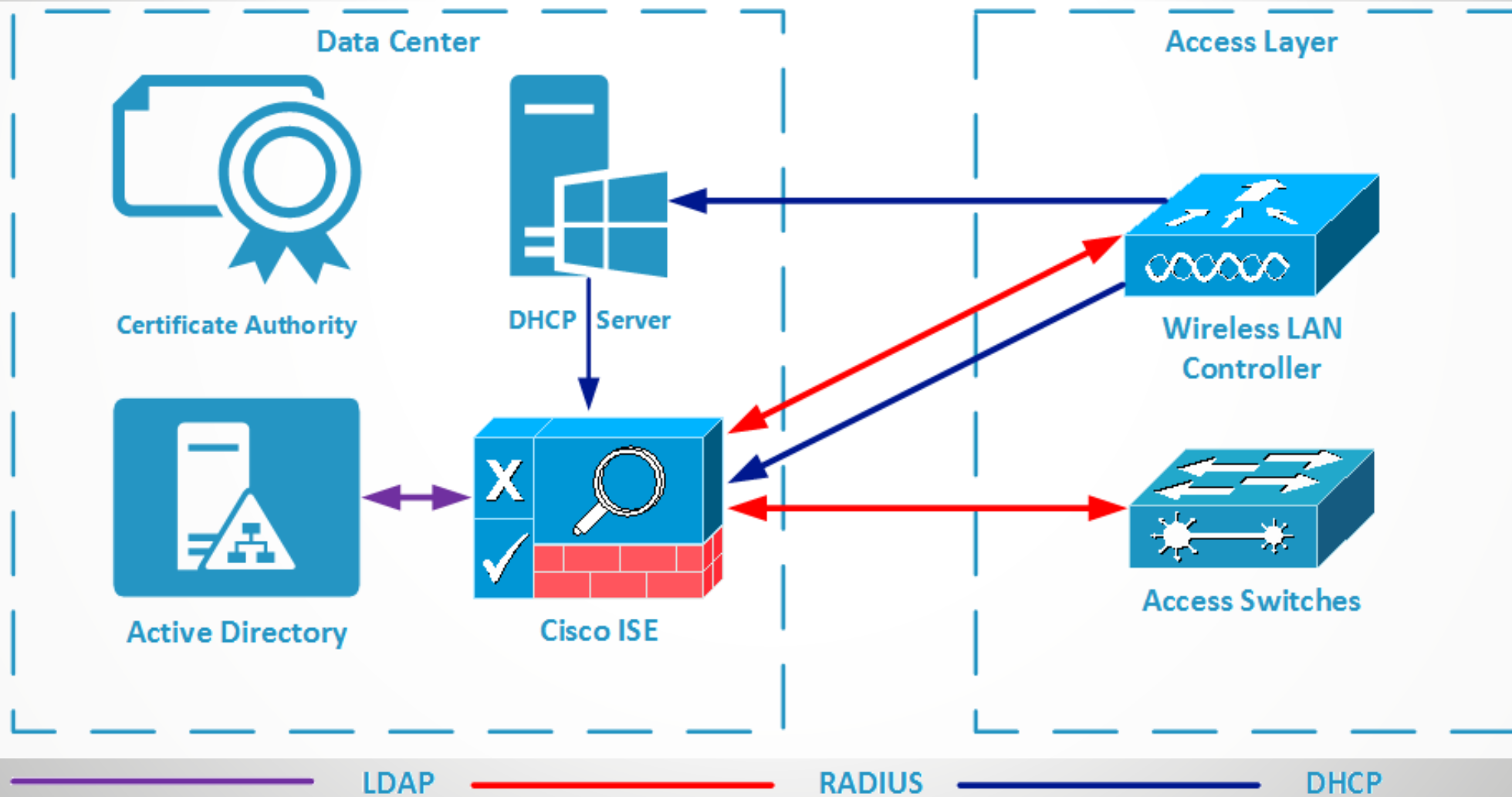
Налаштування та контроль за дотриманням усіх вимог політики доступу до корпоративної мережі з єдиного інтерфейсу

Модель впровадження

Термін	Значення
Service	Функція, яку виконує Persona (доступ до мережі, профілювання, моніторинг та траблшутінг).
Node	Фізичний або віртуальний пристрій Cisco ISE.
Persona	Визначає функції, що надаються Node . Кожна Node може мати наступні Persona : Administration, Policy Service, Monitoring.
Role	Визначає роль standalone, primary або secondary для Administration та Monitoring Node .



Взаємодія з наявною інфраструктурою



Профілювання пристроїв

Cisco ISE Profiler дозволяє:

- Динамічно класифікувати кожен пристрій, що отримує доступ до мережі
- Надає інформацію «Що саме» підключено незалежно від користувача для побудови політик Авторизації на основі типу пристрою.



Cisco ISE Profiler використовує для збору Інформації щодо кінцевих пристроїв:

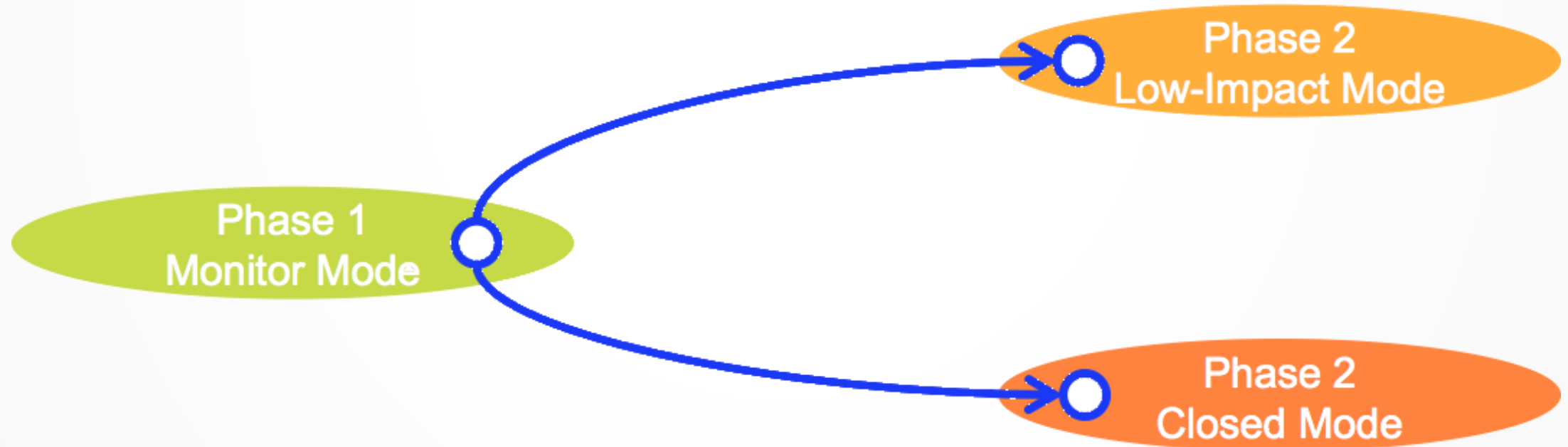
Supported ISE Probes

DHCP	HTTP	SNMP Query
RADIUS	SNMP Trap	DHCP SPAN
DNS	NMAP	NetFlow

Поетапне впровадження системи

З метою мінімізації впливу на користувачів та інфраструктуру впровадження системи контролю доступу до корпоративної мережі розподіляється на 2 основні етапи.

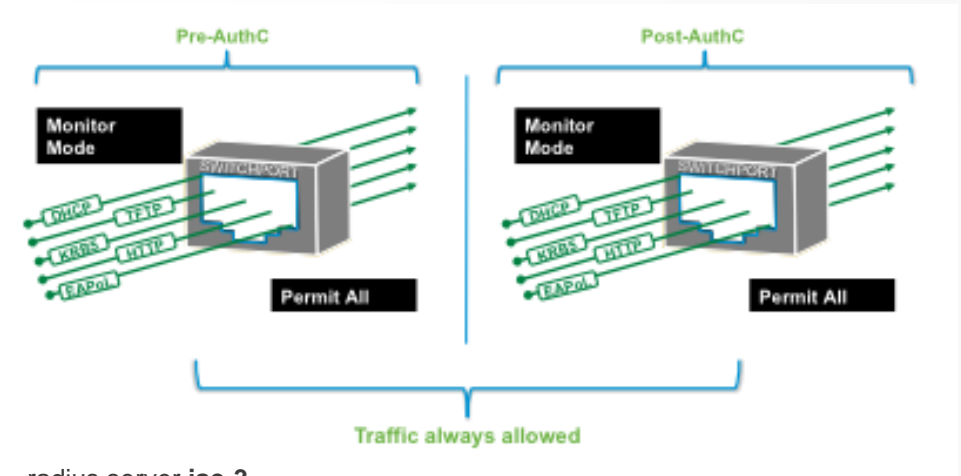
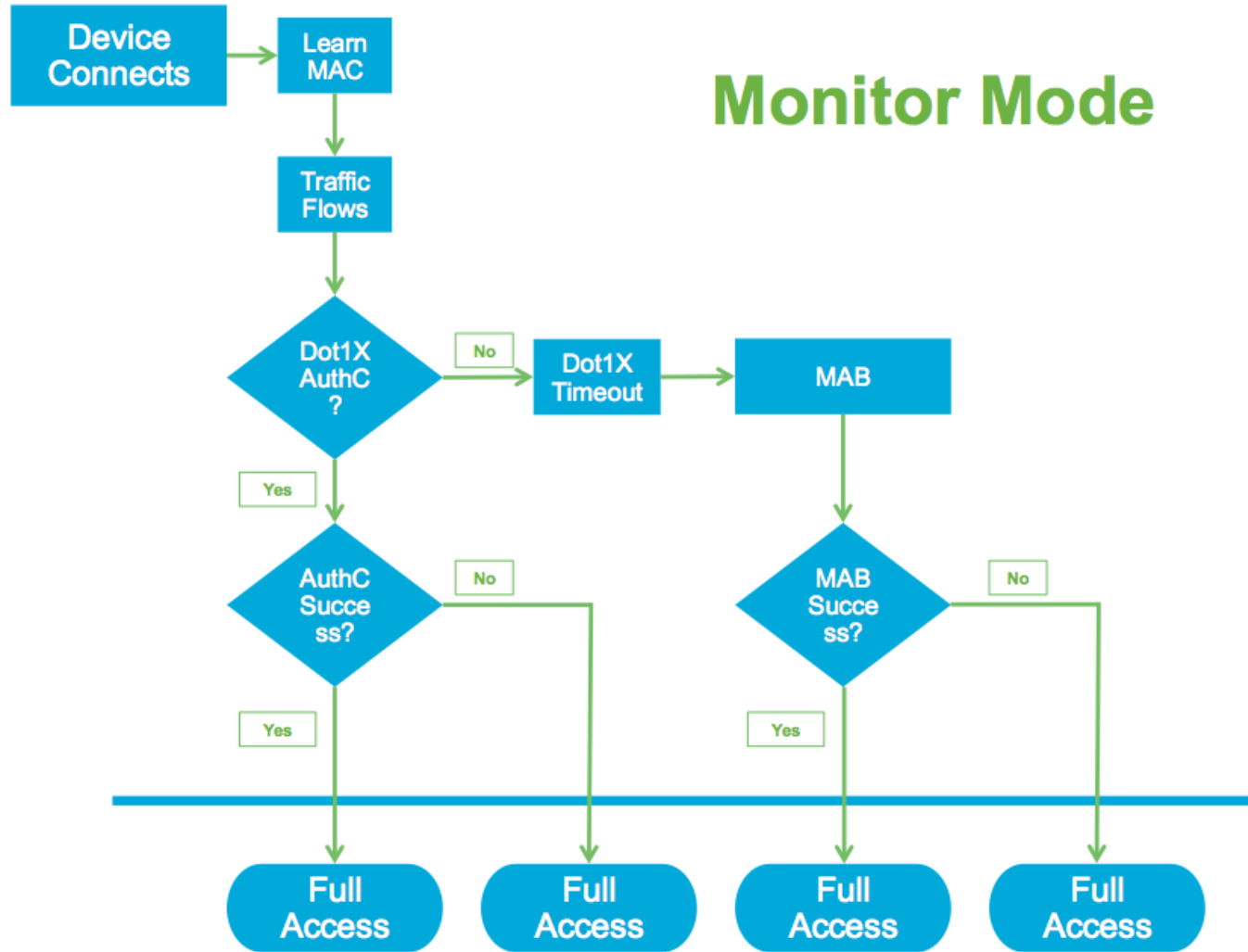
- Етап 1. Monitor Mode – необхідний етап, що дозволяє адміністратору системи вирішити всі проблеми, наглядно показуючи успішні та невдалі спроби автентифікації.



Monitor Mode

Authentication Method

Final Port Status



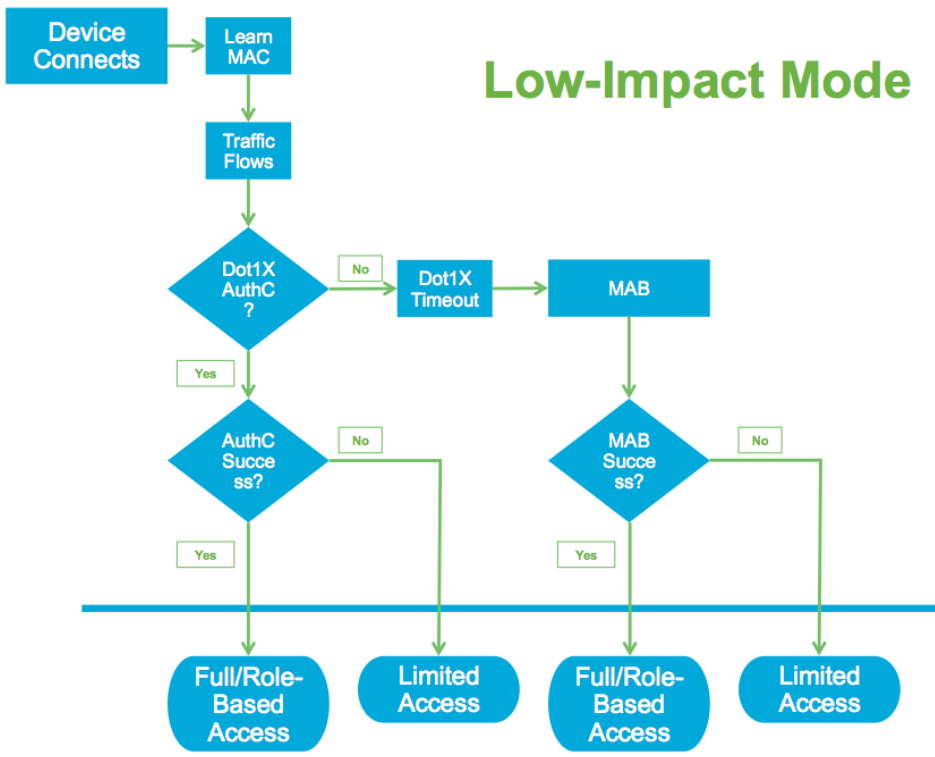
```

radius server ise-3
address ipv4 10.4.48.43 auth-port 1812 acct-port 1813
key [radius key]
radius server ise-4
address ipv4 10.4.48.44 auth-port 1812 acct-port 1813
key [radius key]
aaa group server radius ISE_GROUP
server name ise-3
server name ise-4
aaa authentication dot1x default group ISE_GROUP
aaa authorization network default group ISE_GROUP
aaa authorization configuration default group ISE_GROUP
aaa accounting dot1x default start-stop group ISE_GROUP
radius-server vsa send accounting
radius-server vsa send authentication
  
```

Low-Impact or Closed Mode

Authentication Method

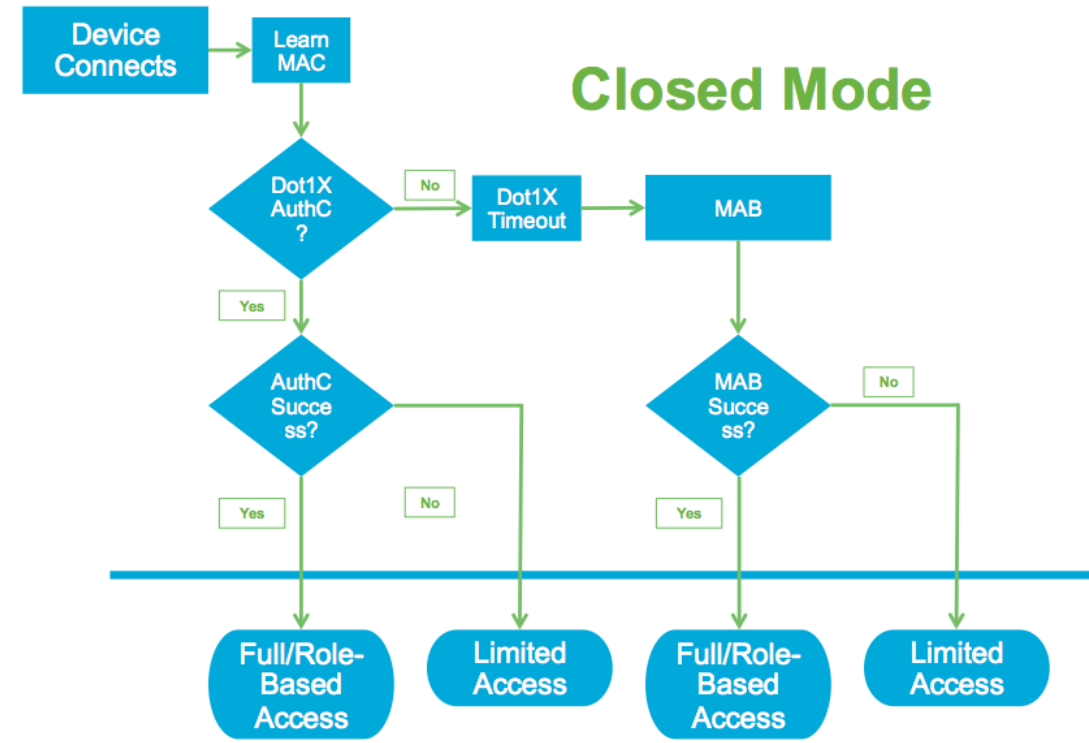
Low-Impact Mode



OR

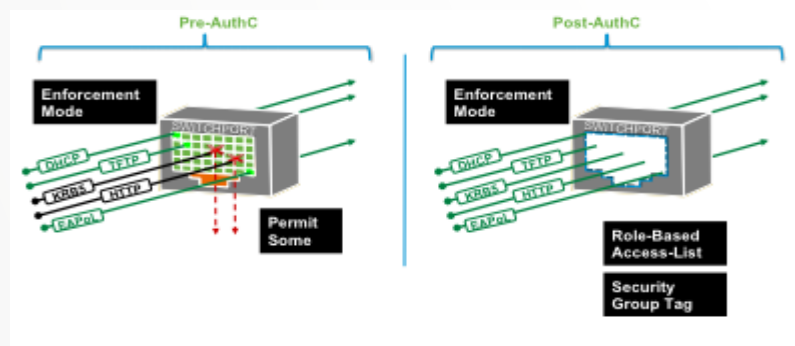
Authentication Method

Closed Mode

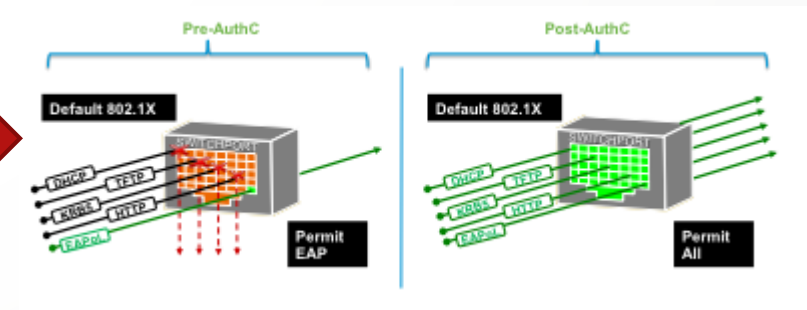


Final Port Status

Final Port Status



Switchport



Profiler Policy

Profiling

←
≡
⚙️

- Profiling Policies
- Logical Profiles
 - Cameras
 - Gaming Devices
 - Home Network Devices
 - IP-Phones
 - Infrastructure Network Devices
 - Medical Devices
 - Mobile Devices
 - Printers

Profiler Policy List > **Cisco-IP-Phone-7821**

Profiler Policy

* Name Description

Policy Enabled

* Minimum Certainty Factor (Valid Range 1 to 65535)

* Exception Action

* Network Scan (NMAP) Action

Create an Identity Group for the policy Yes, create matching Identity Group
 No, use existing Identity Group hierarchy

* Parent Policy

* Associated CoA Type

System Type Cisco Provided

Rules

If Condition Then

If Condition Then

If Condition Then

Context Visibility

Cisco Identity Services Engine
Home | Context Visibility | Operations | Policy | Administration | Work Centers

Endpoints | Network Devices

Authentication
BYOD
Compliance
Compromised Endpoints
Endpoint Classification
Guest
Vulnerable Endpoints

ENDPOINTS

Type | Profile

ENDPOINT CATEGORIES

OUI | OS Types | Identity Group

NETWORK DEVICES

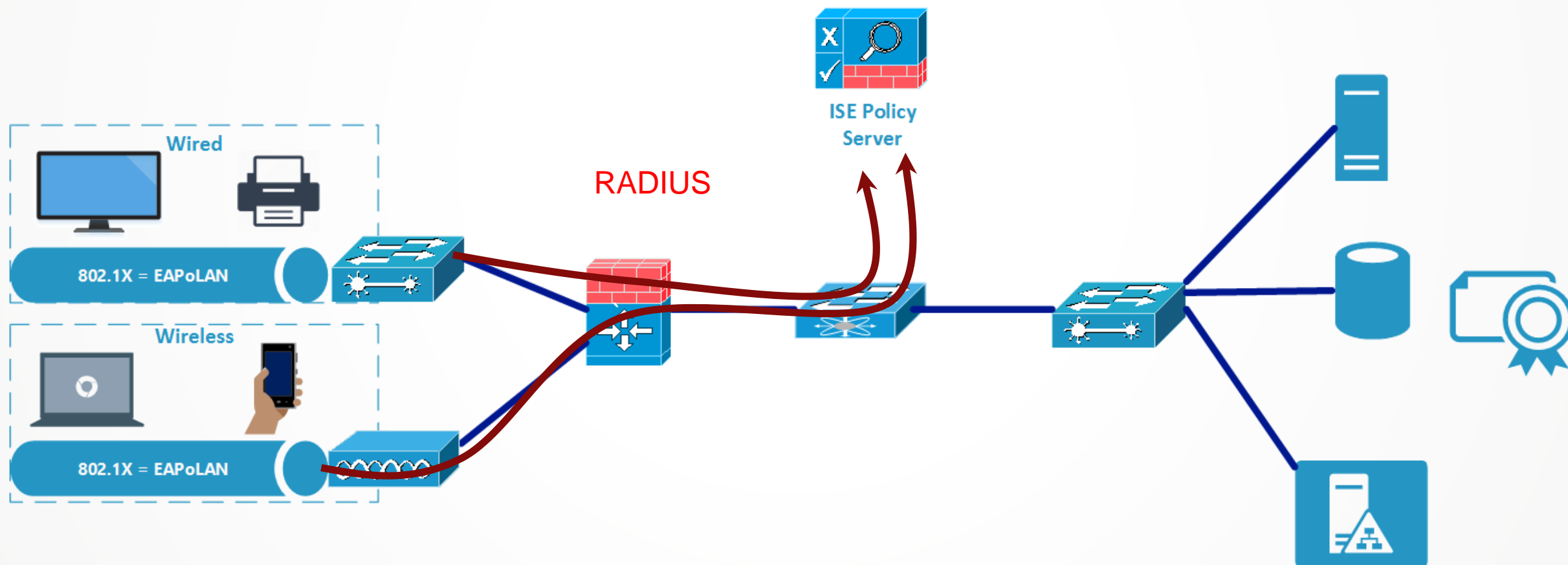
Location | Type | Device Name

Rows/Page 50 / 2 / 760 Total Rows

Refresh
+ Add
Trash
Edit
ANC
Change Authorizaton
Clear Threats & Vulnerabilities
Export
Import
MDM Actions
Revoke Certificate

<input type="checkbox"/>	MAC Address	IPv4 Address	Username	Hostname	Location	Endpoint Profile	Description	OUI	OS Types	Status
<input checked="" type="checkbox"/>	<input type="text" value="MAC Address"/>	<input type="text" value="IPv4 Address"/>	<input type="text" value="Username"/>	<input type="text" value="Hostname"/>	<input type="text" value="Location"/>	<input type="text" value="Endpoint Profile"/>	<input type="text" value="Description"/>	<input type="text" value="OUI"/>	<input type="text" value="OS Types"/>	<input type="text" value="Status"/>

Підтримка Cisco та сторонніх рішень використовуючи стандартні протоколи: RADIUS, 802.1X, EAP



Політики авторизації та автентифікації



Policy Sets

Search policy names & descriptions.

Summary of Policies

- Global Exceptions
- Wireless_Partner
- Wired_Thin
- Wireless_Corp
- Wired_Corp**

Save Order Reset Order

Набори політик

Умови даного набору політик

Політики автентифікації

Політики авторизації

Define the Policy Sets by configuring rules based on conditions. Drag and drop sets on the left hand side to change the order. For Policy Export go to Administration > System > Backup & Restore > Policy Export Page

Status	Name	Description	Conditions	Permissions
✓	Wired_Corp		DEVICE:Device Type EQUALS Device Type#All Device Types#Access-layer#C3850-48U	

Authentication Policy

- ✓ MAB : If Wired_MAB OR Wireless_MAB Allow Protocols : Default Network Access and
- ✓ Default : use Internal Endpoints
- ✓ Dot1X : If Wired_802.1X... Allow Protocols : Default Network Access and
- ✓ EAP-TLS_Machine : if Network Access:EapAuthenticati Use Dot1X_Machine_Certs
- ✓ EAP-TLS_Phones : if Network Access:EapAuthenticati Use Dot1X_Phones
- ✓ Default : Use example.com

Authorization Policy

Exceptions (0)

Standard

Status	Rule Name	Conditions (identity groups and other conditions)	Permissions
✓	Wired Dot1X Endpoints	if Wired_802.1X	then Wired_Dot1X
✓	Wireless Dot1X Endpoints	if Wireless_802.1X	then Wireless_Dot1X
✓	Wireless Black List Default	if Blacklist AND Wireless_Access	then Blackhole_Wireless_Access
✓	Profiled Cisco IP Phones	if Cisco-IP-Phone	then Cisco_IP_Phones
✓	Profiled Non Cisco IP Phones	if Non_Cisco_Profiled_Phones	then Non_Cisco_IP_Phones

Identity Source: example.com

Options

- If authentication failed: Reject
- If user not found: Reject
- If process failed: Drop

Note: For authentications using PEAP, LEAP, EAP-FAST, EAP-TLS or RADIUS MSCHAP it is not possible to continue processing when authentication fails or user is not found. If continue option is selected in these cases, requests will be rejected.

	ISE Posture Agent for Windows	Web Agent for Windows	ISE Posture Agent for Macintosh OS X
Умови відповідності	<ul style="list-style-type: none"> Operating System/Service Packs/Hotfixes Service Check Registry Check File Check Application Check Antivirus Installation Antivirus Version/ Antivirus Definition Date Antispyware Installation Patch Management Check Windows Update Running Windows Update Configuration WSUS Compliance Settings 	<ul style="list-style-type: none"> Operating System/Service Packs/Hotfixes Service Check Registry Check File Check Application Check Antivirus Installation Antivirus Version/ Antivirus Definition Date Antispyware Installation Windows Update Running Windows Update Configuration WSUS Compliance Settings 	<ul style="list-style-type: none"> Service Check File Check Application Check Antivirus Installation Antivirus Version/ Antivirus Definition Date Antispyware Installation
Дії, направлені на приведення до відповідності	<ul style="list-style-type: none"> Message Text (Local Check) URL Link (Link Distribution) File Distribution Launch Program Antivirus Definition Update Antispyware Definition Update Patch Management Remediation Windows Update WSUS 	<ul style="list-style-type: none"> Message Text (Local Check) URL Link (Link Distribution) File Distribution 	<ul style="list-style-type: none"> Message Text (Local Check) URL Link (Link Distribution) Antivirus Live Update Antispyware Live Update

Автентифікація ноутбуків працівників
використовуючи цифрові сертифікати
Microsoft CA

SSID: CORP



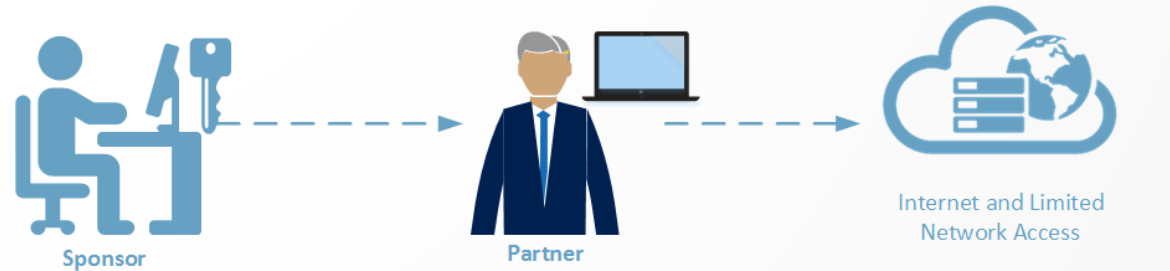
Миттєвий доступ без паролю через Hotspot
Portal

SSID: Guest



Контрольований доступ партнерів за
допомогою Self-registration та Sponsor Portals

SSID:
SPONSORED



Swatch A – вигляд за замовчуванням

Swatch B – вигляд елементів при наведенні на них (наприклад, кнопка Асцепт)

Swatch C – визначає елементи, такі як сповіщення, повідомлення про помилки, недійсні поля введення тощо

The screenshot displays the ThemeRoller jQuery Mobile interface. On the left, the 'Swatch A' configuration panel is visible, showing settings for Page, Header/Footer Bar, Body, Link, and Button: Normal. The main area shows three columns of UI components corresponding to Swatch A, Swatch B, and Swatch C. Swatch A (Global) shows a light theme with grey and white colors. Swatch B (A) shows a dark theme with blue and black colors. Swatch C (C) shows a light theme with red and white colors. The components include Body, List Header, List items, Radio and Checkbox controls, On/Off toggles, Option 1 dropdowns, Text Input fields, and Buttons.

Результати впровадження

Надано інформацію в реальному часі щодо того «хто», «що», «коли», «звідки» та «яким чином» отримав доступ до мережі

Реалізовано гнучкий механізм контролю доступу до мережі та механізм захисту від неконтрольованого доступу

Забезпечено контроль відповідності пристроїв до мережі заданим критеріям, автоматизовано ізоляцію пристроїв, що не відповідають їм та процес приведення до відповідності

Забезпечено ефективну сегментацію мережі

Надання механізму керування життєвим циклом гостьового та партнерського WI-FI доступу

Дякую за увагу!