Guest/BYOD WIFI
Central Authentication and Accounting management

Aim of this solution:

* To create a one-stop ‘self service’ portal for the creation of Guest and Visitor accounts by a company employee (sponsors). Each account will provide access to the public internet on ALL sites equipped with Cisco guest Wi-Fi facilities across the region (WebAUTH).
* To allow internet access for BYOD’s of a company Employees across the region with 802.1x using AD authentication and AD Group control.

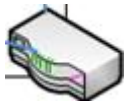
The Building Blocks

http://xxxx
Web Front end
Radius Server
SQL dB

Corporate WAN

Internet

Location A

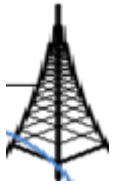


WIFI Controller

SSID: 1234

SSID: 1234BYOD

SSID: 1234GUEST



Access Point

BYOD User

Company
Owner/Sponsor

Guest User

1234GUEST

STEP1 . Company user goes to the self service Portal URL and creates a guest account

http://xxxx

Web Front end
Radius Server
SQL dB

Corporate WAN

Internet

Location A

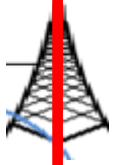
WIFI Controller

SSID: 1234

SSID: 1234BYOD

SSID: 1234GUEST

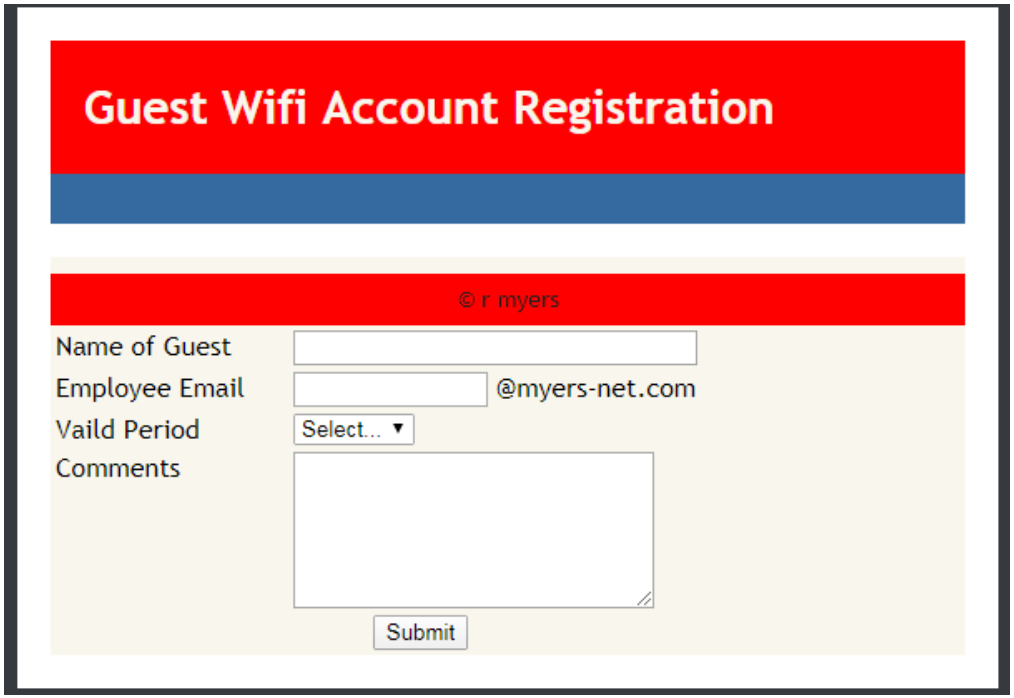
BYOD User



Access Point

Company
Owner/Sponsor

Guest User


Guest Wifi Account Registration
© r myers
Name of Guest
Employee Email
@myers-net.com
Vaild Period
Select...
Comments
Submit

1234GUEST

STEP2 . Company user receives an email containing the username and password of the guest account

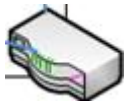
http://xxx

Web Front end
Radius Server
SQL dB

Corporate WAN

Internet

Location A

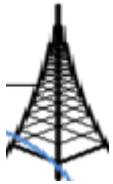


WIFI Controller

SSID:1234

SSID:1234BYOD

SSID: 1234GUEST

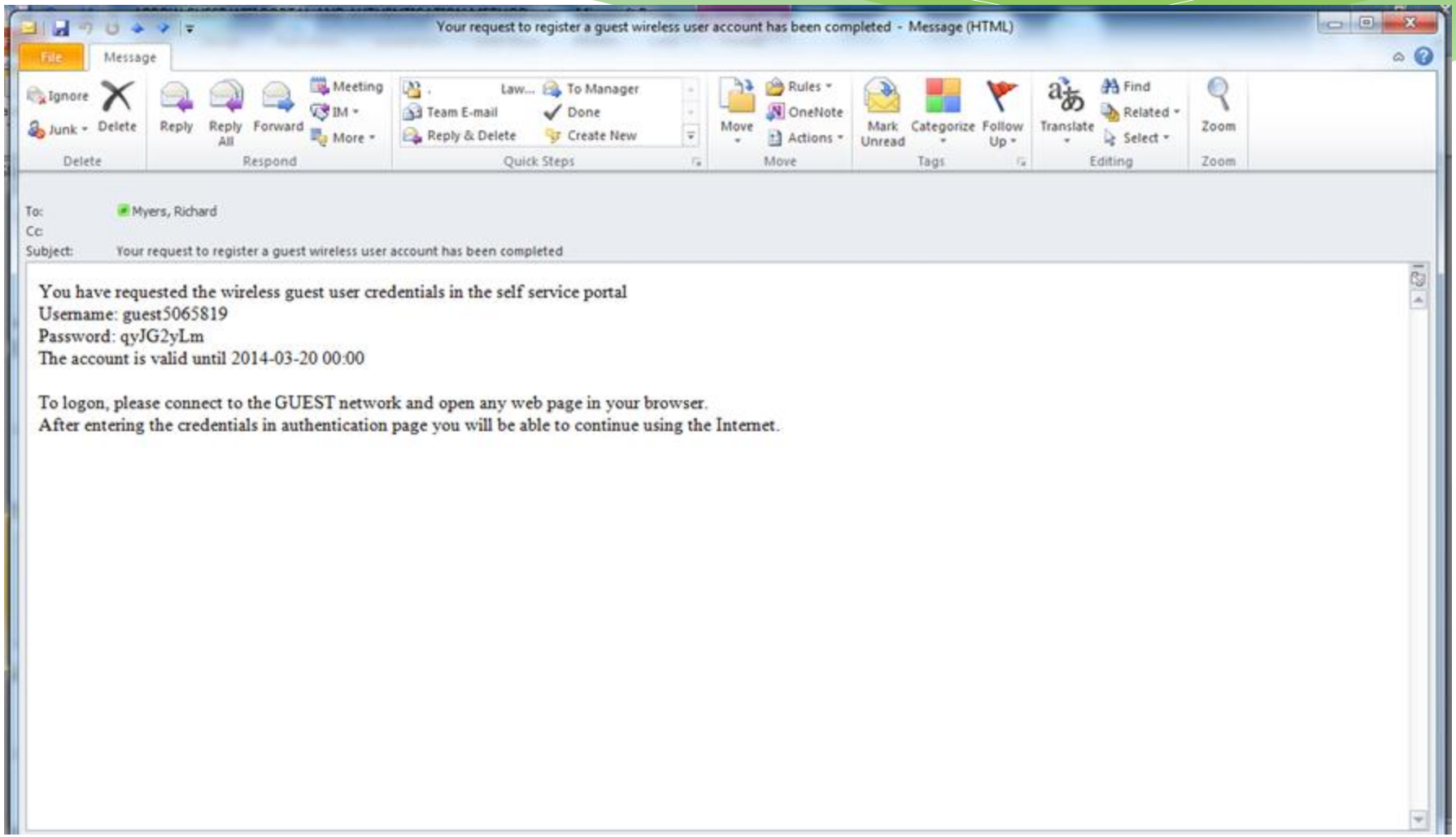


Access Point

BYODUser

Company
Person/Sponsor

Guest User

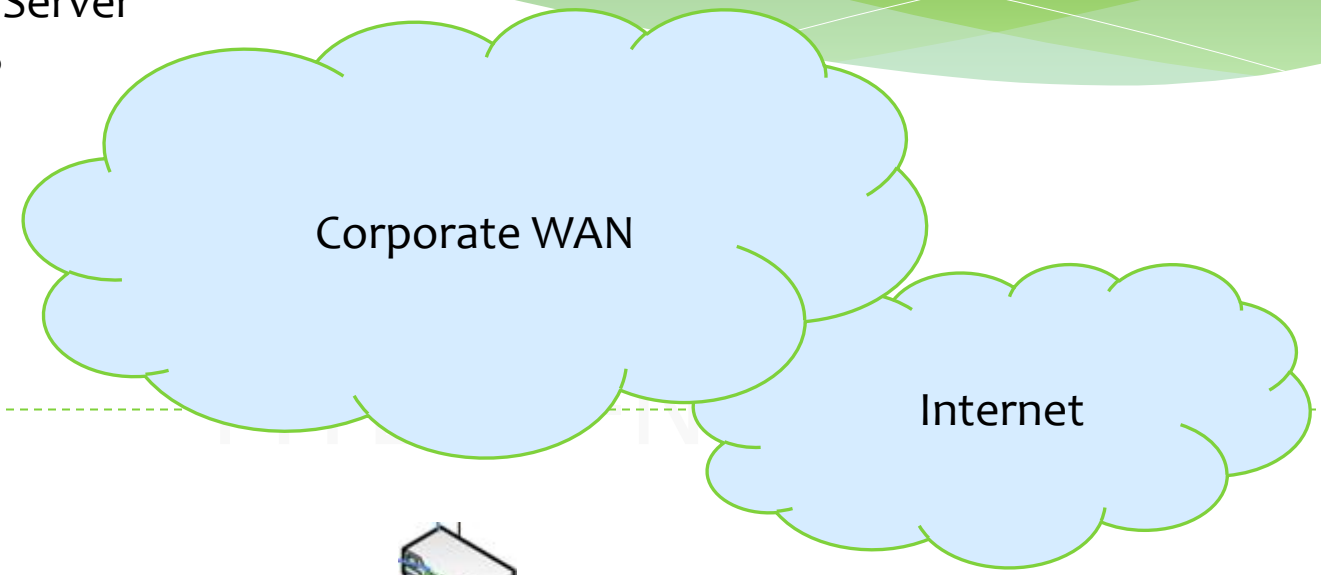

Your request to register a guest wireless user account has been completed - Message (HTML)
File
Message
Ignore
Junk
Delete
Reply
Reply All
Forward
Meeting
IM
More
Team E-mail
Reply & Delete
To Manager
Done
Create New
Move
Rules
OneNote
Actions
Mark Unread
Categorize
Follow Up
Translate
Find
Related
Select
Zoom
Delete
Respond
Quick Steps
Move
Tags
Editing
Zoom
To: Myers, Richard
Cc:
Subject: Your request to register a guest wireless user account has been completed
You have requested the wireless guest user credentials in the self service portal
Username: guest5065819
Password: qyJG2yLm
The account is valid until 2014-03-20 00:00
To logon, please connect to the GUEST network and open any web page in your browser.
After entering the credentials in authentication page you will be able to continue using the Internet.

1234GUEST

STEP3 . Company user passes on the information to the guest

http://xxxxx

Web Front end
Radius Server
SQL dB



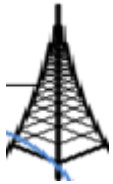
Location A

WIFI Controller

SSID:1234

SSID: 1234BYOD

SSID: 1234GUEST



Access Point

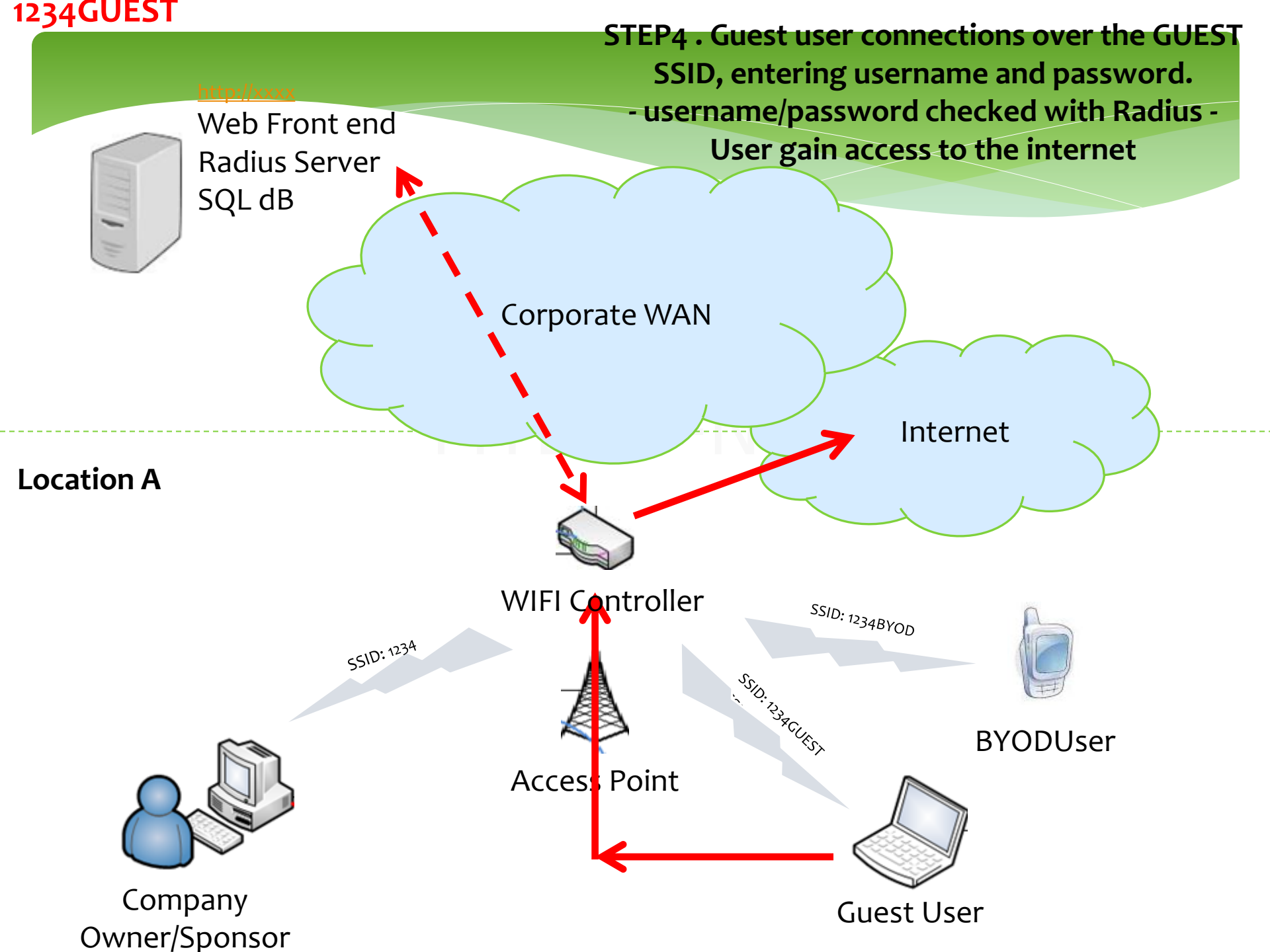
MDLZ User

Company
Owner/Sponsor

Guest User

1234GUEST

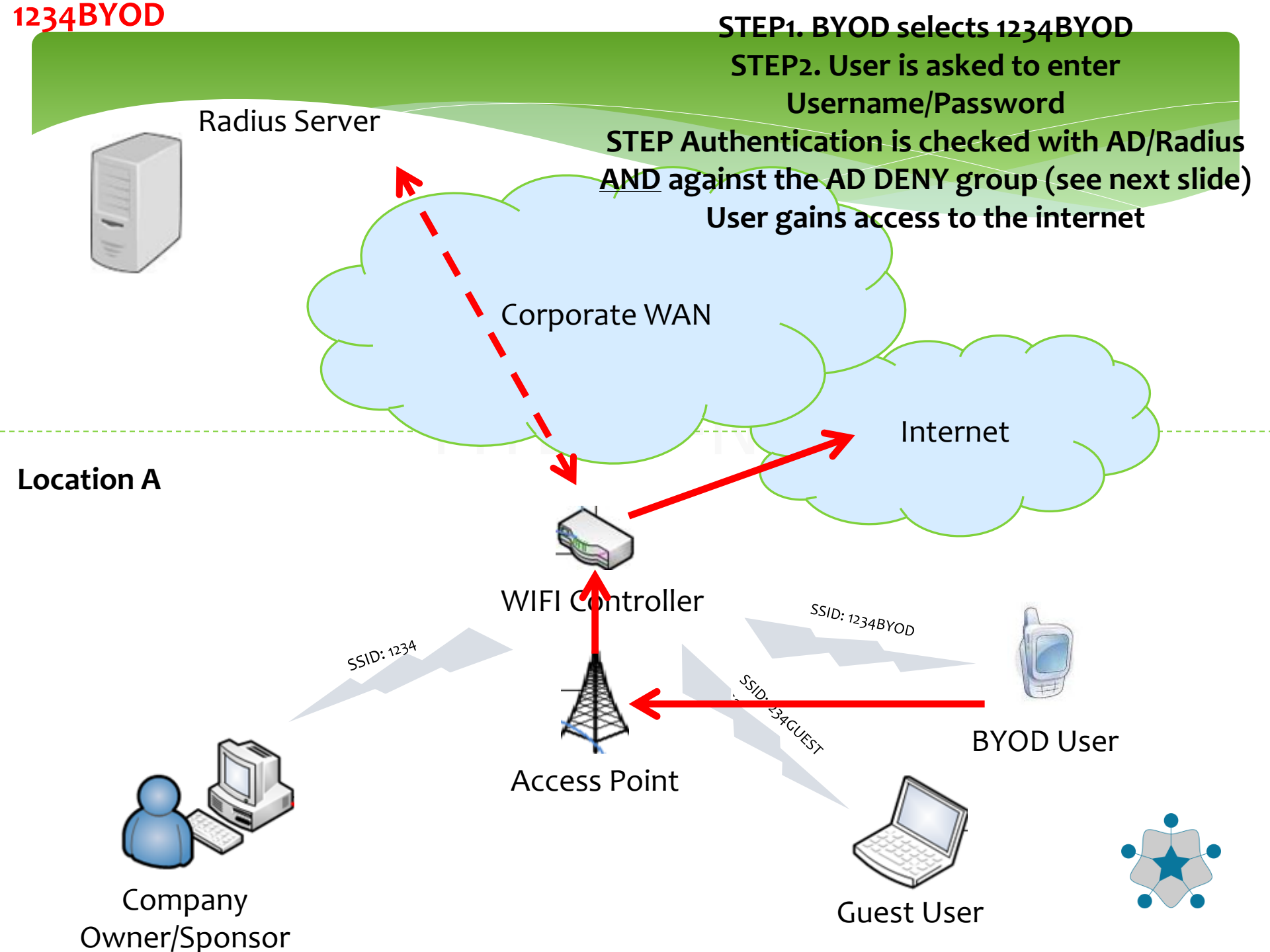
STEP4 . Guest user connections over the GUEST SSID, entering username and password.
- username/password checked with Radius -
User gain access to the internet



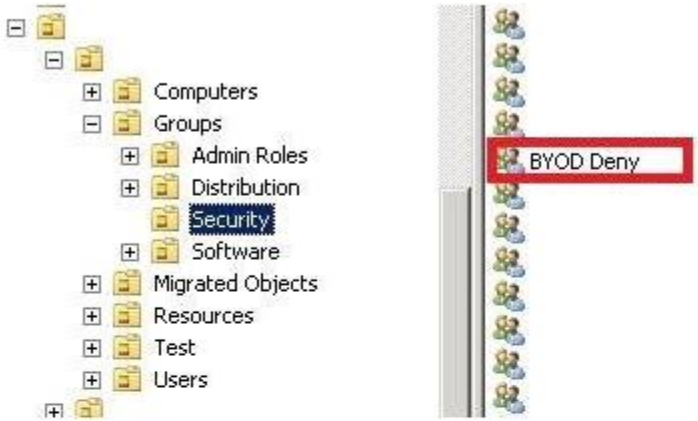
1234GUEST

Features

* Same account can be used in across the whole region (if the account is still active).
* Logging of the guess account is tied to the company sponsor in case of abuse of misuse.
* Flexibility in terms of account age.
* Cross-platform compatible web-based authentication when the user opens any URL in the browser
* simple fit for purpose solution

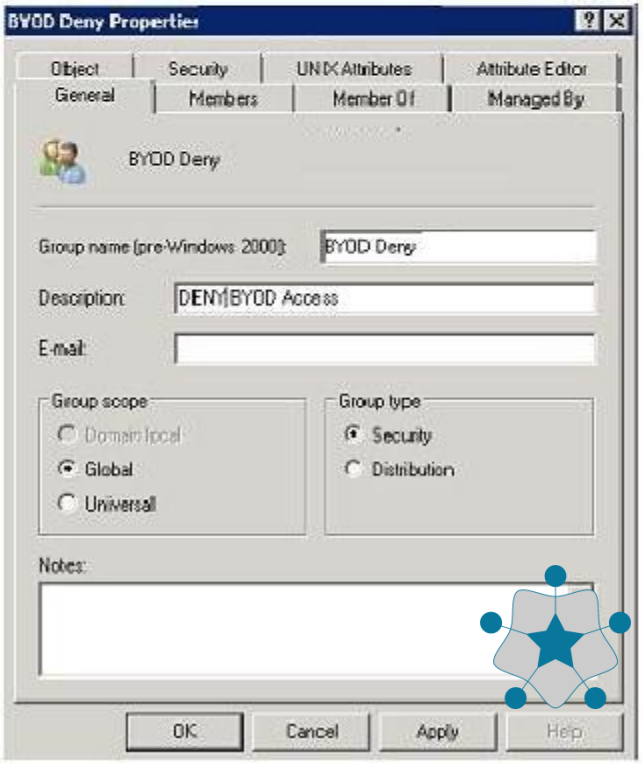

1234BYOD
STEP1. BYOD selects 1234BYOD
STEP2. User is asked to enter Username/Password
STEP Authentication is checked with AD/Radius AND against the AD DENY group (see next slide)
User gains access to the internet
Radius Server
Corporate WAN
Internet
Location A
WIFI Controller
SSID: 1234
SSID: 1234BYOD
SSID: 1234GUEST
Access Point
BYOD User
Company Owner/Sponsor
Guest User

Simple guide to managing BYOD DENY for Employees



1. Open up the Active Directory and locate your security Container within your country and site

2. Find the Group name BYOD Deny and then add a user who should NOT be able to access internet with their BYOD



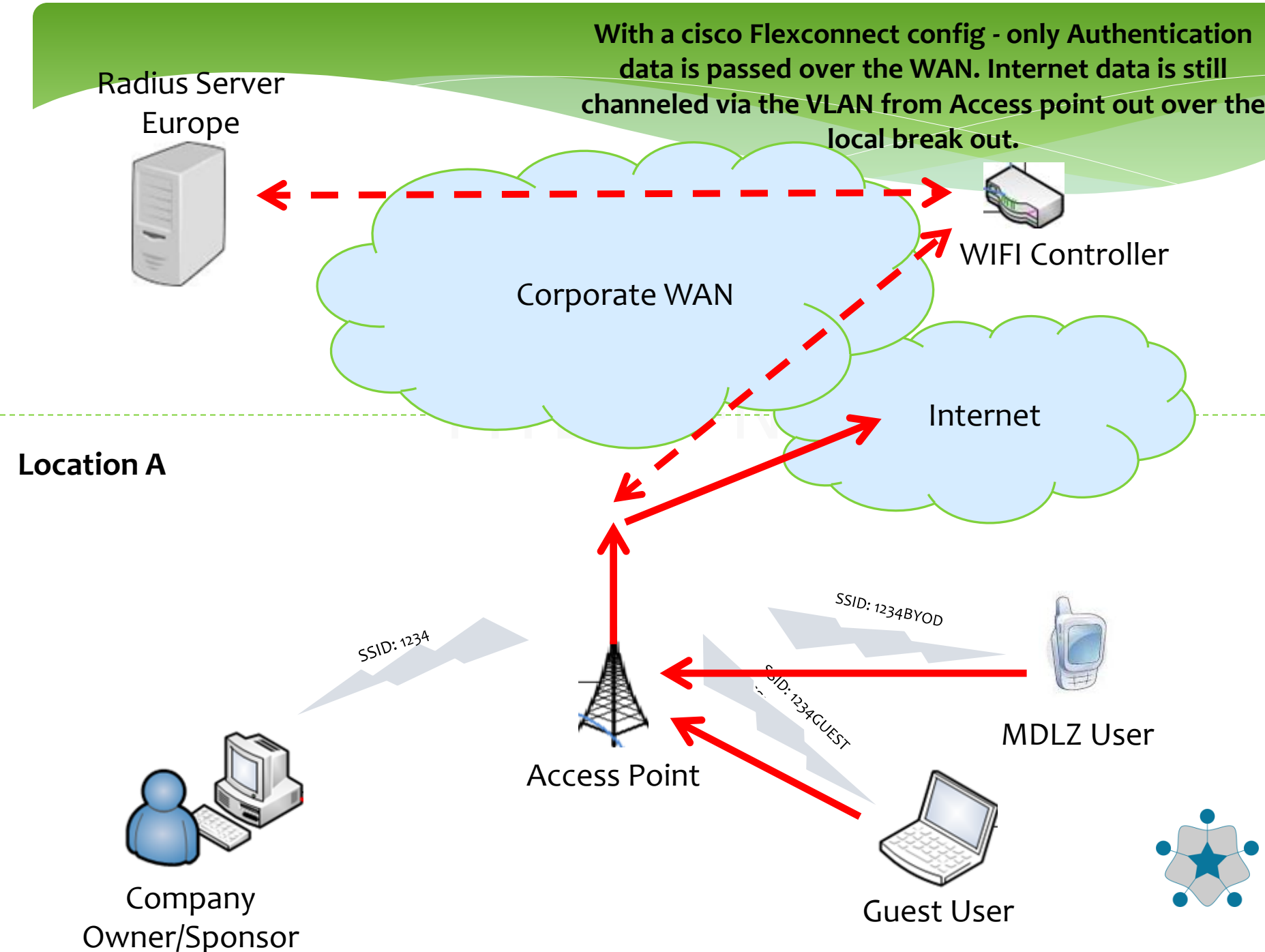
In order to control which users can use BYODWIFI and more importantly to prevent internet BW flooding we apply a AD Deny group option. Anyone who is a member of this group (ex. blue collar workers) will not automaticity have access to the BYODWIFI

Features

* Easy of use through the users normal AD domain account “logon and play”.
* Additional security by the use of AD groups to manage who can access with BYOD to control excess usage of WAN BW and abuse.

Other Regions with Central Controllers

FLEXCONNECT – Central WLC's



Authentication Method

* **Guest WEBAUTH**

laptops do not need to have their profiles setup manually. Enter Credentials and go. No loss of connection after device ‘sleep mode’ kicks in if the WLC firmware is above version 7.5

* **BYOD 802.1x**

Phones would retain credentials in cache. For company notebook users local profile needs to be setup.