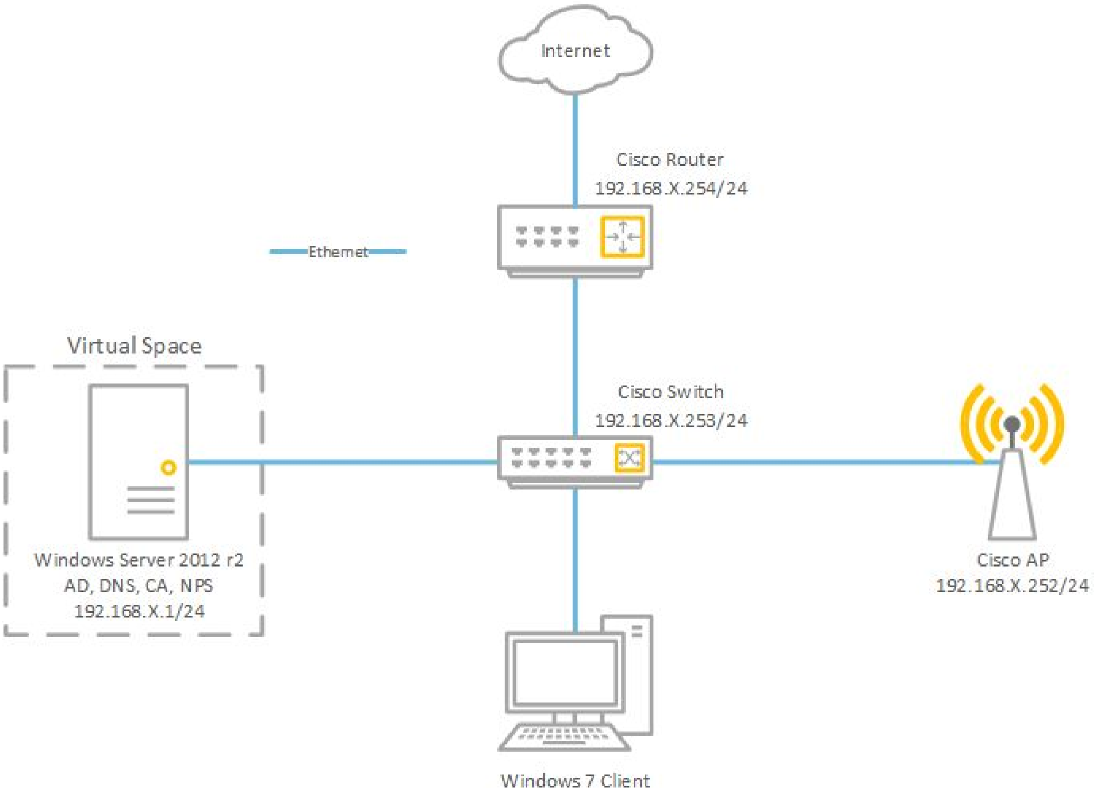
AD and RADIUS Introduction

Active Directory (AD) is software available on Microsoft Windows server platforms. AD provides a means to centralize the management of users and computers within a domain. Users and computers within AD can be assigned to groups and groups can be assigned to groups. These AD objects are organized into logical groups which are called Organizational Units (OU). Group Policies allow for different permissions to be assigned to users, computers or groups. This enables you the powerful ability to assign specific permissions to each object.

Remote Authentication Dial-IN User Service (RADIUS) is a standard protocol that allows for centralized Authentication, Authorization and Accounting (AAA) management for who and/or what can connect to a network or use a network service. RADIUS can easily be integrated with AD to allow a systems administrator to easily manage who and/or what is using their network.

Final Topology



Router & Switch Setup

1. Write erase and reload router
2. Assign interface fastethernet 0/1 the IP address of 192.168.X.254/24 and connect it to the switch
    a. Make sure the port on the switch is configured as an access port, not dynamic
    b. Everything should be one one LAN/VLAN on the switch
3. Configure interface fastethernet 0/0 to get an DHCP address from the lab and connect it to a DHCP port
4. Configure a DHCP for your LAN and exclude 192.168.X.1; .252; .253; .254;
    a. .254 - router
    b. .253 - switch vlan1
    c. .252 - ap
    d. .1 - server
5. Configure NAT so your can get to the internet

Active Directory Setup

1. Ensure the ***Windows Server 2012 R2*** virtual machine network interface is set to bridge mode and boot it up
2. Assign a static IP of ***192.168.X.1/24*** where is your bench number
3. Launch ***Add Roles and Features*** within Server Manager
4. Select defaults and on the Server Roles page select ***Active Directory Domain Servers***
    a. Make sure you install DNS with AD
5. Once installation is complete, promote server to a domain controller by addressing the flag in Server Manager
6. Create a ***new forest*** with a unique name ending in .edu
7. Ensure DNS server is selected on DC Options page and enter password for DSRM
8. Leave defaults for the rest and install
9. Launch ***Active Directory Users and Computers*** and create a new user Organizational Unit and then create new user within the OU
10. Join a Windows 7 computer to the domain
11. Login to the Windows 7 client using domain credentials
    a. Something you keep in mind - how does the client know about the AD server?

Install & Configure Roles Need for RADIUS

1. Launch ***Add Roles and Features*** within Server Manager
2. Select defaults and on the Server Roles page select ***Active Directory Certificate Servers*** and ***Network Policy and Access Services***
3. Select defaults for the rest and install
4. ‘Configure’ Active Directory Certificate Service from alert dropdown on Server Manager
5. Select ***Certificate Authority***
6. Select ***Standalone CA***
7. Select ***Root CA***
8. Select ***Create New Private Key***
9. Leave the rest of the prompts as default until you can select ***Configure***
10. Launch NPS within Server Manager
11. Right click on NPS (Local) and ***register with Active Directory***

Network Policy Server Setup for Cisco Device

1. Create a new RADIUS Client for your Router
    a. Under the **Settings Tab** → ***Select Enable this Radius client***
    b. Enter a ***friendly name*** for your router
    c. Enter the ***IP Address*** of the router
    d. Select ***None*** from the drop down under Shared Secret
    e. Select ***Manual*** and enter a Shared Secret
    f. Under the **Advanced Tab** → Select ***Cisco*** from the Vendor drop down menu
2. Create a Network Policy under Policies
    a. Enter a policy name, and select **Unspecified** under the Type of Network Access Server
    b. Under Policy Conditions add the *special* group of users for your domain
    c. Under Access Permissions select ***Access Granted***
    d. Under Authentication Methods <u>uncheck</u> all boxes except for ***Unencrypted Authentication (PAP, SPAP)***
    e. Leave the Constraints section as default
    f. Under Configure Settings under standard remove the default attributes and add a ***Service-Type*** set to ***Login***
    g. Next edit the ***Vendor Specific*** settings
    h. Add an attribute for ***Cisco-AV-Pair*** with the vendor selected as ***Cisco*** and configure the value EXACTLY as follows ***shell:priv-lvl=15***
    i. Click ***Next*** and then ***Finish***

<u>Cisco Device Configuration for RADIUS Authentication</u> (see *Appendix A* for more hints)

1. Enable *aaa new-model*
2. Configure a *aaa group* for your radius server
3. Create *aaa authentication*, *authorization*, and *accounting* methods and tie these to your aaa group
4. Set the radius server, auth-port, and acct-port as well as a key
5. Set your vty line to use your aaa authorization and authentication methods
6. Set your vty line to allow both telnet and ssh

<u>Create Certificate for Server Validation with Wireless Clients</u>

1. Search for Microsoft Management Console (MMC)
2. Select File → Add/Remove snap in
3. Add Certificates
4. Right Personal and select All Tasks → Request new certificate
5. Select Active directory Enrollment Policy
6. Select Administrator
7. Under Details → select Properties and create a friendly name

<u>Network Policy Server Setup for Wireless Clients</u>

1. Create a new RADIUS Client for your Access Point
    a. Under the **Settings Tab** → ***Select Enable this Radius client***
    b. Enter a ***friendly name*** for your Access Point
    c. Enter the ***IP Address*** of the Access Point
    d. Select ***None*** from the drop down under Shared Secret
    e. Select ***Manual*** and enter a Shared Secret
    f. Under the **Advanced Tab** → Select ***Cisco*** from the Vendor drop down menu
2. Create a new Standard Configuration Policy for 802.1X
    a. Navigate to ***NPS Local*** Tree
    b. Select ***RADIUS server for 802.1X Wireless or Wired Connections*** from dropdown
    c. Select ***Configure 802.1X***
    d. Select ***Secure Wireless Connections***, hit next
    e. Ensure your previously created RADIUS clients are added, hit next
    f. On Authentication Method select ***Microsoft: Protected EAP (PEAP)*** from the dropdown and hit configure
    g. Ensure the certificate you created previously is selected and <u>not</u> your root certificate
    h. Select ***Okay*** and ***Next***
    i. Add the *special* group for users of your domain
    j. Hit ***Next*** through the rest of the defaults until ***Finish***

<u>Access Point Setup</u> (See *Appendix B* for hints)

1. Make sure to wipe existing configuration on your AP (*write erase* and *reload* commands)
2. Very similar to your Router and Switch aaa setup:
    a. Enable *aaa new-model*
    b. Create a *aaa* radius server group with the IP of your Radius server
    c. Create *aaa* authentication, authorization, and accounting methods tied to your *aaa* radius server group
    d. Assign an IP address of 192.168.1.252 to your *BVI1* (bridge virtual interface) - this will be used to allow the AP to communicate with a radius server
    e. Create an *ssid* with the following configuration at a minimum:
        i. Authentication open eap and network eap
        ii. Key-management WPAv2
        iii. Guest-mode
    f. Apply your *ssid* to a radio interface(s)
    g. Set your radio interface(s) to use an encryption mode (tkip will work for WPAv2)
3. Make sure you have a corresponding Network Policy created in your Windows server with the AP as a Radius client
4. Attempt to connect to your wireless network with an account created in AD
5. If your PC will not connect to this wireless network you may need to uncheck “Verify certificate” under the wireless settings for that network in Windows

Appendix A - Cisco aaa command hints

```
aaa new-model
!
!
aaa group server radius [group name]
      server [ip]
!
!
aaa authentication login userAuthentication local group [group name]
aaa authorization exec userAuthorization local group [group name]
if-authenticated
aaa accounting exec default start-stop group [group name]
aaa accounting system default start-stop group [group name]
!
!
radius-server host [ip] auth-port [port] acct-port [port] key [key]
!
!
line vty 0 4
      Authorization exec userAuthorization
      Login authentication userAuthentication
      Transport input telnet ssh
!
!
```

Appendix B - Cisco AP commands

```
aaa new-model
!
aaa group server radius [group name]
      server [ip]
!
!
aaa authentication login userAuthentication group [group name]
!
!
radius-server host [ip] auth-port [port] acct-port [port] key [key]
!
!
ip radius source-interface BVI1
interface BVI1
```

```
      ip address 192.168.1.X 255.255.255.0
!
dot11 ssid [ssid name]
      authentication open eap [group name]
      authentication network-eap [group name]
      authentication key-management wpa version 2
      Guest-mode
      Infrastructure-ssid optional
!
!
interface dot11radio [0 or 1]
      ssid [ssid name]
      encryption mode ciphers tkip
```