Atribuição do VLAN dinâmico com exemplo de configuração NGWC e ACS 5.2

Índice

Introdução

Este documento descreve o conceito da atribuição do VLAN dinâmico. Igualmente descreve como configurar o controlador do Wireless LAN (WLC) e um servidor Radius a fim atribuir clientes do Wireless LAN (WLAN) a um VLAN específico dinamicamente. Neste documento, o servidor Radius é um Access Control Server (ACS) essa versão 5.2 do Cisco Secure Access Control System das corridas.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Conhecimento básico do WLC e do Lightweight Access Points (regaços)

- Conhecimento funcional do server do Authentication, Authorization, and Accounting (AAA)
- Conhecimento completo da rede Wireless e problemas de segurança Wireless

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Controlador do Wireless LAN de Cisco 5760 com software release 3.2.2 do ® XE do Cisco IOS (armário de fiação da próxima geração, ou NGWC)
- Access point do peso leve do 3602 Series do Cisco Aironet
- Microsoft Windows XP com o suplicante de Intel Proset
- Versão 5.2 do Cisco Secure Access Control System
- Cisco Catalyst 3560 Series Switch

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Atribuição da VLAN (Rede local virtual) dinâmica com servidor Radius

Na maioria de sistemas de WLAN, cada WLAN tem uma política estática que se aplica a todos os clientes associados com um Service Set Identifier (SSID), ou o WLAN na terminologia do controlador. Embora poderoso, este método tem limitações porque exige que os clientes se associem com os diferentes SSID para herdar diferentes QoS e políticas de segurança.

Mas a solução de Cisco WLAN suporta identidades na rede. Isto permite a rede anuncie um único SSID, mas permite que os usuários específicos herdem QoS diferente, atributos VLAN, e/ou políticas de segurança baseadas nas credenciais do usuário.

A atribuição da VLAN dinâmica é um recurso que coloca um usuário wireless em uma VLAN específica baseado nas credenciais fornecidas pelo usuário. Esta tarefa da atribuição do usuário a um VLAN específico é segurada por um servidor de autenticação RADIUS, tal como um Cisco Secure ACS. Esta característica pode ser usada, por exemplo, a fim permitir que o host wireless permaneça no mesmo VLAN que move dentro de uma rede do campus.

Em consequência, quando um cliente tenta associar a um REGAÇO registrado com um controlador, o REGAÇO passa as credenciais do usuário ao servidor Radius para a validação. Quando a autenticação é bem sucedida, o servidor Radius passa determinados atributos da Internet Engineering Task Force (IETF) ao usuário. Estes atributos RADIUS decidem a ID da VLAN que deve ser atribuído ao cliente wireless. O SSID do cliente (o WLAN, em termos do WLC) não importa porque o usuário é atribuído sempre a este ID de VLAN predeterminado.

Os atributos do usuário do RADIUS usados para a atribuição de ID da VLAN são:

- IETF 64 (tipo de túnel) - Ajuste ao VLAN.
- IETF 65 (tipo médio do túnel) - ajuste a 802.
- IETF 81 (Túnel-Privado-Grupo-ID) - Ajuste ao ID de VLAN.

O ID de VLAN é 12 bit e toma um valor entre 1 e 4094, inclusivo. Porque o Túnel-Privado-Grupo-

ID é do tipo corda, como definido no RFC 2868, atributos RADIUS para o apoio do protocolo de túnel para o uso com IEEE 802.1X, o valor de número inteiro do ID de VLAN é codificado como uma corda. Quando estes atributos de túnel são enviados, é necessário preencher o campo Tag.

Como é explicado na RFC2868 , seção 3.1:

“O campo da etiqueta é um octeto de comprimento e é pretendido fornecer meios de agrupar os atributos no mesmo pacote que referem o mesmo túnel.”

Os valores válidos para o campo da etiqueta são 0x01 com 0x1F, inclusivo. Se o campo Tag não for utilizado, ele deve ser zero (0x00). Consulte na RFC 2868 mais informações sobre todos os atributos de RADIUS.

Configurar

A configuração de uma atribuição do VLAN dinâmico consiste em duas etapas distintas:

1. Configurar o WLC com o comando line interface(cli) ou com o GUI.
2. Configurar o servidor Radius.

   Note: Use a Command Lookup Tool (somente clientes registrados) para obter mais informações sobre os comandos usados nesta seção.

Diagrama de Rede

Este documento utiliza a seguinte configuração de rede:

Este documento usa o 802.1X com protocolo extensible authentication protegido (PEAP) como o mecanismo de segurança.

Hipóteses

- O Switches é configurado para toda a camada 3 (L3) VLAN.
- O servidor DHCP é atribuído um escopo de DHCP.
- A Conectividade L3 existe entre todos os dispositivos na rede.
- O REGAÇO é juntado já ao WLC.
- Cada VLAN tem uma máscara de /24.
- O ACS 5.2 tem um certificado auto-assinado instalado.

Configurar o WLC com CLI

Configurar o WLAN

Este é um exemplo de como configurar um WLAN com o SSID de DVA:

```
wlan DVA 3 DVA
 aaa-override
 client vlan VLAN0020
 security dot1x authentication-list ACS
 session-timeout 1800
 no shutdown
```

Configurar o servidor Radius no WLC

Este é um exemplo da configuração do servidor Radius no WLC:

```
aaa new-model
!
!
aaa group server radius ACS
 server name ACS
!
aaa authentication dot1x ACS group ACS

radius server ACS
 address ipv4 10.106.102.50 auth-port 1645 acct-port 1646
 key Cisco123

dot1x system-auth-control
```

Configurar o conjunto de DHCP para o cliente VLAN

Este é um exemplo da configuração do conjunto de DHCP para o VLAN 30 do cliente e o VLAN 40:

```
interface Vlan30
 ip address 30.30.30.1 255.255.255.0
!
interface Vlan40
 ip address 40.40.40.1 255.255.255.0

ip dhcp pool vla30
 network 30.30.30.0 255.255.255.0
 default-router 30.30.30.1
!
ip dhcp pool vlan40
 network 40.40.40.0 255.255.255.0
 default-router 40.40.40.1

ip dhcp snooping vlan 30,40
ip dhcp snooping
```

Configurar o WLC com GUI

Configurar o WLAN

Este procedimento descreve como configurar o WLAN.

1. Navegue à **configuração** > ao **Sem fio** > ao **WLAN** > aba **NOVA**.

2. Clique o **tab geral** a fim ver que o WLAN está configurado para WPA2-802.1X, e traçar a relação/grupo de Interfrace (G) a VLAN20 (**VLAN0020**).

3. Clique o **guia avançada**, e verifique a caixa de verificação da **ultrapassagem reservar AAA**. A ultrapassagem deve ser permitida para que esta característica trabalhe.

4. Clique a **ABA de segurança** e a aba **Layer2**, verifique WPA2 a caixa de verificação da criptografia **AES**, e selecione o **802.1x da** lista de drop-down de Mgmt da chave do AUTH.

Configurar o servidor Radius no WLC

Este procedimento descreve como configurar o servidor Radius no WLC.

1. Navegue à aba do > segurança da **configuração**.

2. Navegue a **AAA > grupos de servidor > raio** a fim criar os grupos de servidor Radius. Neste exemplo, o grupo de servidor Radius é chamado ACS.

3. Edite a entrada do servidor Radius a fim adicionar o endereço IP do servidor e o segredo compartilhado. Este segredo compartilhado deve combinar o segredo compartilhado no WLC e no servidor Radius.

   Este é um exemplo de uma configuração completa:

Configurar o servidor Radius

Este procedimento descreve como configurar o servidor Radius.

1. No servidor Radius, navegue aos **usuários e a identidade armazena > identidade interna armazena > usuários**.

2. Crie os nomes de usuário e os grupos apropriados da identidade. Neste exemplo, é

estudante e todos os grupos: Estudantes, e professor e AllGroups: Professores.

3. Navegue aos **elementos da política >** à **autorização e às permissões >** aos **perfis do acesso de rede >** da **autorização**, e crie os perfis da autorização para a ultrapassagem AAA.

4. Edite o perfil da autorização para o estudante.

5. Ajuste o VLAN ID/Name como a **estática** com um valor de **30** (VLAN 30).

6. Edite o perfil da autorização para o professor.

7. Ajuste o VLAN ID/Name como a **estática** com um valor de **40** (VLAN 40).

8. Navegue às **políticas de acesso >** ao **acesso presta serviços de manutenção > acesso de rede padrão**, e clicam a aba **permitida dos protocolos**. Verifique a caixa de seleção **reservar PEAP**.

9. Navegue à **identidade**, e defina as regras a fim permitir usuários PEAP.

10. Navegue à **autorização**, e o estudante e o professor do mapa à política da autorização; neste exemplo, o mapeamento deve ser estudante para o VLAN 30 e professor para VLAN 40.

Verificar

Use esta seção para confirmar se a sua configuração funciona corretamente. Estes são os processos de verificação:

- Monitore a página no ACS esse as mostras que os clientes são autenticados.

- Conecte ao DVA WLAN com o grupo de estudantes, e reveja a utilidade da conexão de WiFi do cliente.

- Conecte ao DVA WLAN com o grupo do professor, e reveja a utilidade da conexão de WiFi do cliente.

Troubleshooting

Esta seção fornece informações que podem ser usadas para o troubleshooting da sua configuração.

> Notas:
>
> Use a Command Lookup Tool (somente clientes registrados) para obter mais informações sobre os comandos usados nesta seção.
>
> A ferramenta Output Interpreter (clientes registrados somente) apoia determinados comandos de exibição. Use a ferramenta Output Interpreter a fim ver uma análise do emissor de comando de execução.
>
> Consulte Informações Importantes sobre Comandos de Depuração antes de usar comandos **debug**.

Útil debuga incluem **debugam o** *Mac do* **endereço MAC de cliente**, assim como os estes comandos trace NGWC:

- **o nível ajustado do grupo-Sem fio-cliente do traço debuga**
- **ajuste o Mac** *xxxx.xxxx.xxxx do* **filtro do grupo-Sem fio-cliente do traço**
- **mostre SYS-filtrar-traços do traço**

O traço NGWC não inclui dot1x/AAA, assim que use esta lista inteira de traços combinados para dot1x/AAA:

- **o nível ajustado do grupo-Sem fio-cliente do traço debuga**
- **o nível ajustado do evento do traço wcm-dot1x debuga**
- **o nível ajustado do traço wcm-dot1x aaa debuga**
- **os eventos wireless aaa do traço ajustado em nível debugam**
- **o nível ajustado manutenção programada do núcleo da acesso-sessão do traço debuga**
- **o dot1x ajustado do método da acesso-sessão do traço em nível debuga**
- **ajuste o Mac** *xxxx.xxxx.xxxx do* **filtro do grupo-Sem fio-cliente do traço**
- **ajuste o Mac** *xxxx.xxxx.xxxx do* **filtro do evento do traço wcm-dot1x**
- **ajuste o Mac** *xxxx.xxxx.xxxx do* **filtro do traço wcm-dot1x aaa**
- **ajuste o Mac wireless** *xxxx.xxxx.xxxx do* **filtro dos eventos aaa do traço**

- ajuste o Mac *xxxx.xxxx.xxxx do* filtro manutenção programada do núcleo da acesso-sessão do traço
- ajuste o Mac *xxxx.xxxx.xxxx do* filtro do dot1x do método da acesso-sessão do traço
- mostre SYS-filtrar-traços do traço

Quando a atribuição do VLAN dinâmico está trabalhando corretamente, você deve ver que este tipo de saída do debuga:

```
09/01/13 12:13:28.598 IST 1ccc 5933] 0021.5C8C.C761 1XA: Received Medium tag (0)
Tunnel medium type (6) and Tunnel-Type tag (0) and Tunnel-type (13)
Tunnel-Private-Id (30)
[09/01/13 12:13:28.598 IST 1ccd 5933] 0021.5C8C.C761 Tunnel-Group-Id is 30
[09/01/13 12:13:28.598 IST 1cce 5933] 0021.5C8C.C761 Checking Interface
Change - Current VlanId: 40 Current Intf: VLAN0040 New Intf: VLAN0030 New
GroupIntf:  intfChanged: 1
[09/01/13 12:13:28.598 IST 1ccf 5933] 0021.5C8C.C761 Incrementing the
Reassociation Count 1 for client (of interface VLAN0040)
 --More--         [09/01/13 12:13:28.598 IST 1cd0 5933] 0021.5C8C.C761
Clearing Address 40.40.40.2 on mobile
[09/01/13 12:13:28.598 IST 1cd1 5933] 0021.5C8C.C761 Applying new AAA override
for station  0021.5C8C.C761
[09/01/13 12:13:28.598 IST 1cd2 5933] 0021.5C8C.C761 Override values (cont..)
dataAvgC: -1, rTAvgC: -1, dataBurstC: -1, rTimeBurstC: -1
    vlanIfName: 'VLAN0030', aclName: ''

[09/01/13 12:13:28.598 IST 1cd3 5933] 0021.5C8C.C761 Clearing Dhcp state for
station  ---
[09/01/13 12:13:28.598 IST 1cd4 5933] 0021.5C8C.C761 Applying WLAN ACL policies
to client
[09/01/13 12:13:28.598 IST 1cd5 5933] 0021.5C8C.C761 No Interface ACL used for
Wireless client in WCM(NGWC)
[09/01/13 12:13:28.598 IST 1cd6 5933] 0021.5C8C.C761 Inserting AAA Override
struct for mobile
   MAC:  0021.5C8C.C761 , source 4

[09/01/13 12:13:28.598 IST 1cd7 5933] 0021.5C8C.C761 Inserting new RADIUS
override into chain for station  0021.5C8C.C761
[09/01/13 12:13:28.598 IST 1cd8 5933] 0021.5C8C.C761 Override values (cont..)
dataAvgC: -1, rTAvgC: -1, dataBurstC: -1, rTimeBurstC: -1
   vlanIfName: 'VLAN0030', aclName: ''

 --More--         [09/01/13 12:13:28.598 IST 1cd9 5933] 0021.5C8C.C761
Applying override policy from source Override Summation:

[09/01/13 12:13:28.598 IST 1cda 5933] 0021.5C8C.C761 Override values (cont..)
dataAvgC: -1, rTAvgC: -1, dataBurstC: -1, rTimeBurstC: -1
   vlanIfName: 'VLAN0030', aclName: ''

[09/01/13 12:13:28.598 IST 1cdb 5933] 0021.5C8C.C761 Applying local bridging
Interface Policy for station  0021.5C8C.C761  - vlan 30, interface 'VLAN0030'
[09/01/13 12:13:28.598 IST 1cdc 5933] 0021.5C8C.C761 1XA: Setting reauth timeout
to 1800 seconds from WLAN config
[09/01/13 12:13:28.598 IST 1cdd 5933] 0021.5C8C.C761 1XA: Setting reauth timeout
to 1800 seconds
[09/01/13 12:13:28.598 IST 1cde 5933] 0021.5C8C.C761 1XK: Creating a PKC PMKID
Cache entry (RSN 1)
[09/01/13 12:13:28.598 IST 1cdf 5933] 0021.5C8C.C761 1XK: Set Link Secure: 0


[09/01/13 12:08:59.553 IST 1ae1 5933] 0021.5C8C.C761 1XA: Received Medium tag (0)
Tunnel medium type (6) and Tunnel-Type tag (0) and Tunnel-type (13)
```

Tunnel-Private-Id (40)
[09/01/13 12:08:59.553 IST 1ae2 5933] 0021.5C8C.C761 Tunnel-Group-Id is 40
 --More-- [09/01/13 12:08:59.553 IST 1ae3 5933] 0021.5C8C.C761
Checking Interface Change - Current VlanId: 20 Current Intf: VLAN0020 New Intf:
VLAN0040 New GroupIntf: intfChanged: 1
[09/01/13 12:08:59.553 IST 1ae4 5933] 0021.5C8C.C761 Applying new AAA override for
station 0021.5C8C.C761
[09/01/13 12:08:59.553 IST 1ae5 5933] 0021.5C8C.C761 Override values (cont..)
dataAvgC: -1, rTAvgC: -1, dataBurstC: -1, rTimeBurstC: -1
**   vlanIfName: 'VLAN0040', aclName: ''**

[09/01/13 12:08:59.553 IST 1ae6 5933] 0021.5C8C.C761 Clearing Dhcp state for
station ---
[09/01/13 12:08:59.553 IST 1ae7 5933] 0021.5C8C.C761 Applying WLAN ACL policies
to client
[09/01/13 12:08:59.553 IST 1ae8 5933] 0021.5C8C.C761 No Interface ACL used for
Wireless client in WCM(NGWC)
[09/01/13 12:08:59.553 IST 1ae9 5933] 0021.5C8C.C761 Inserting AAA Override struct
for mobile
   MAC: 0021.5C8C.C761 , source 4

[09/01/13 12:08:59.553 IST 1aea 5933] 0021.5C8C.C761 Inserting new RADIUS override
into chain for station 0021.5C8C.C761
[09/01/13 12:08:59.553 IST 1aeb 5933] 0021.5C8C.C761 Override values (cont..)
dataAvgC: -1, rTAvgC: -1, dataBurstC: -1, rTimeBurstC: -1
   vlanIfName: 'VLAN0040', aclName: ''
 --More--
[09/01/13 12:08:59.553 IST 1aec 5933] 0021.5C8C.C761 Applying override policy
from source Override Summation:

[09/01/13 12:08:59.553 IST 1aed 5933] 0021.5C8C.C761 Override values (cont..)
dataAvgC: -1, rTAvgC: -1, dataBurstC: -1, rTimeBurstC: -1
   vlanIfName: 'VLAN0040', aclName: ''

[09/01/13 12:08:59.553 IST 1aee 5933] 0021.5C8C.C761 Applying local bridging
Interface Policy for station 0021.5C8C.C761 - vlan 40, interface 'VLAN0040'
[09/01/13 12:08:59.553 IST 1aef 5933] 0021.5C8C.C761 1XA: Setting reauth timeout
to 1800 seconds from WLAN config
[09/01/13 12:08:59.553 IST 1af0 5933] 0021.5C8C.C761 1XA: Setting reauth timeout
to 1800 seconds
[09/01/13 12:08:59.553 IST 1af1 5933] 0021.5C8C.C761 1XK: Creating a PKC PMKID
Cache entry (RSN 1)