Cisco ISE — Autenticação MAB e 802.1X

Fernando Mantovani Pierobon · Follow
Published in TechRebels · 7 min read · Jan 28, 2020

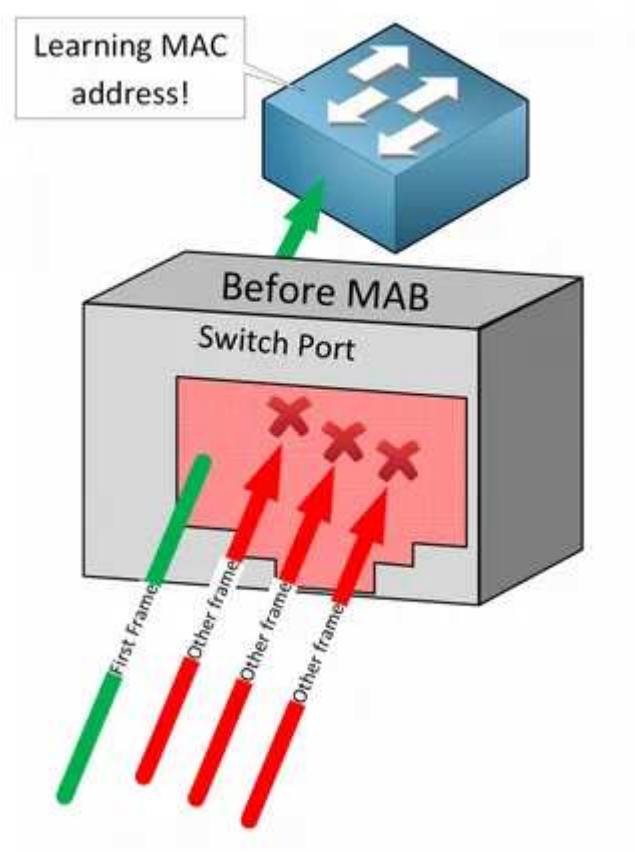
Lab de ISE com MAB e 802.1X

Tudo bem pessoal?

Após conhecermos um pouco do ISE e fazermos um tour pelas principais funcionalidades (acesse aqui os artigos anteriores: ISE Basics — Parte 1 e ISE Basics — Parte 2), vamos agora logo para o que interessa! **Faremos duas configurações de autenticação básicas de MAB e 802.1x.**

Primeiro as definições:

- MAB que é o acrônimo de *Mac Authentication Bypass:* é um mecanismo que permite a integração de equipamentos que não suportam 802.1x se autenticarem na rede.

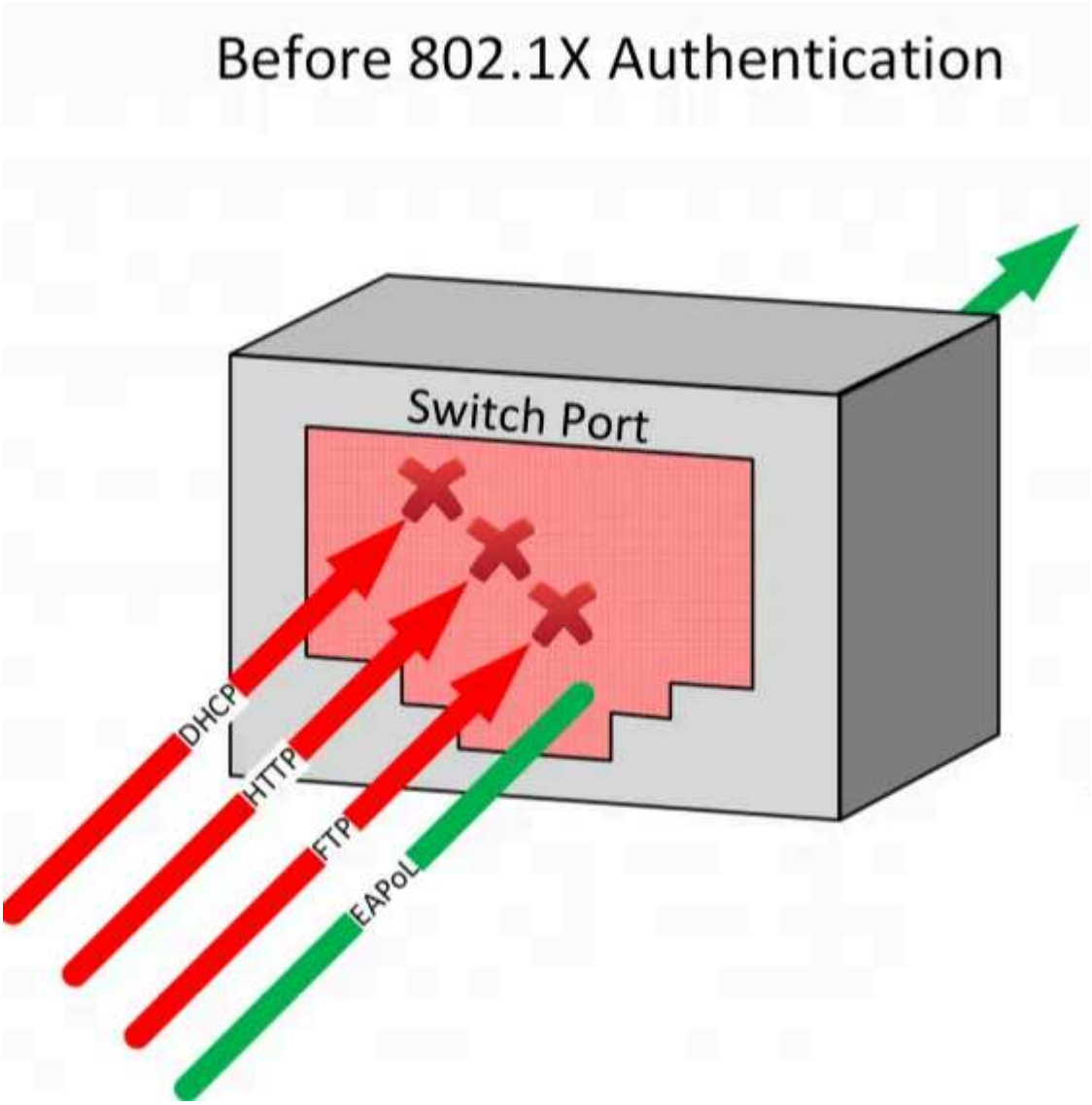


Quando habilitamos o MAB numa porta do switch, essa porta libera apenas o primeiro pacote (para aprender o endereço MAC), ficando todos os outros bloqueados até que a autenticação ocorra.

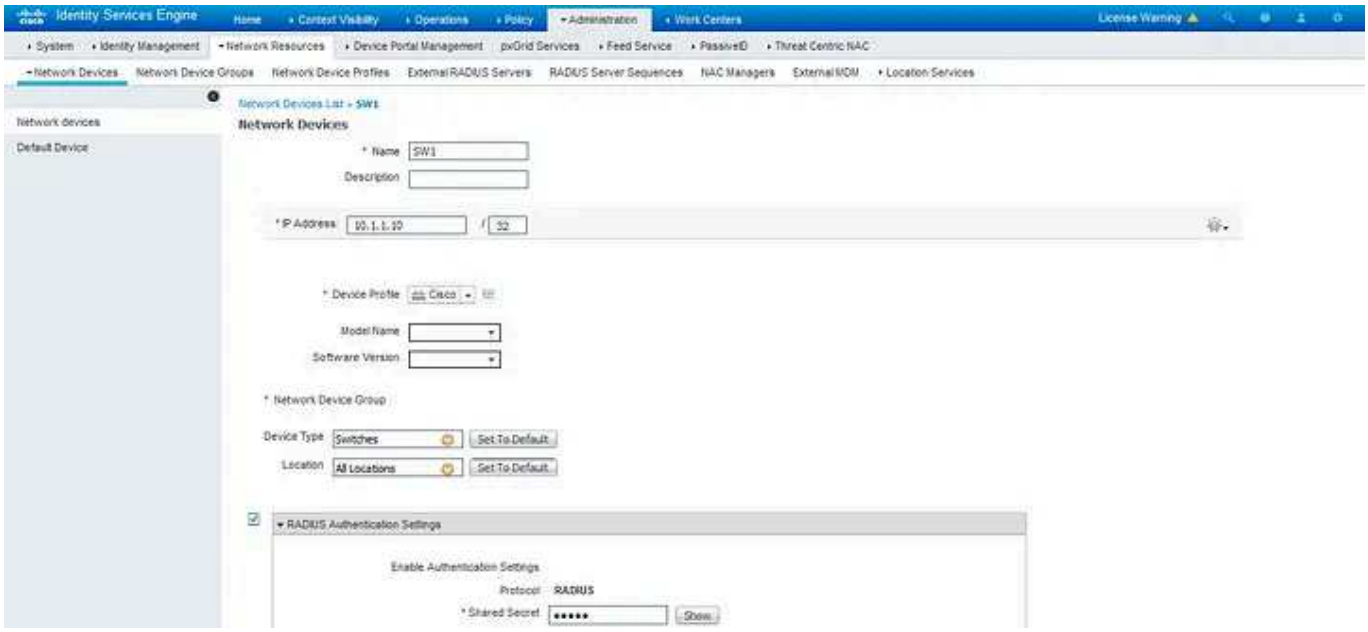
Ele não é um mecanismo muito seguro, já que é fácil ***spoofar*** um MAC, portanto, muitas vezes é utilizado como fallback do 802.1x.

- 802.1x, às vezes chamado de Dot1x, é um protocolo padrão IEEE para controle de acesso à rede. Ele faz parte do grupo IEEE 802.1 de protocolos de redes de computadores. A IEEE 802.1x define o encapsulamento do *Extensible Authentication Protocol* (EAP) sobre IEEE 802, que é conhecido como "*EAP over LAN*" ou **EAPOL**. Isso significa que qualquer

computador que tentar se conectar à rede, deverá primeiro fornecer informações de autenticação.

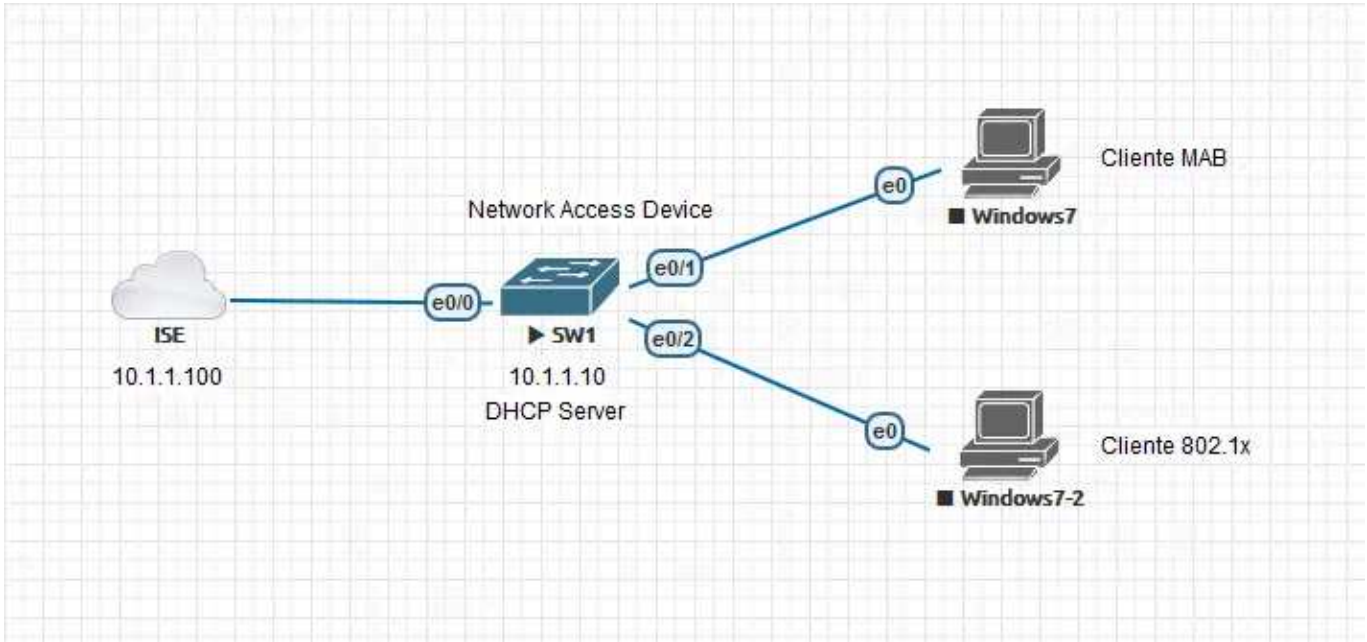


Relembrando, no artigo passado (novamente o link está aqui: ISE Basics — Parte 2), nós fizemos a configuração do switch no ISE.

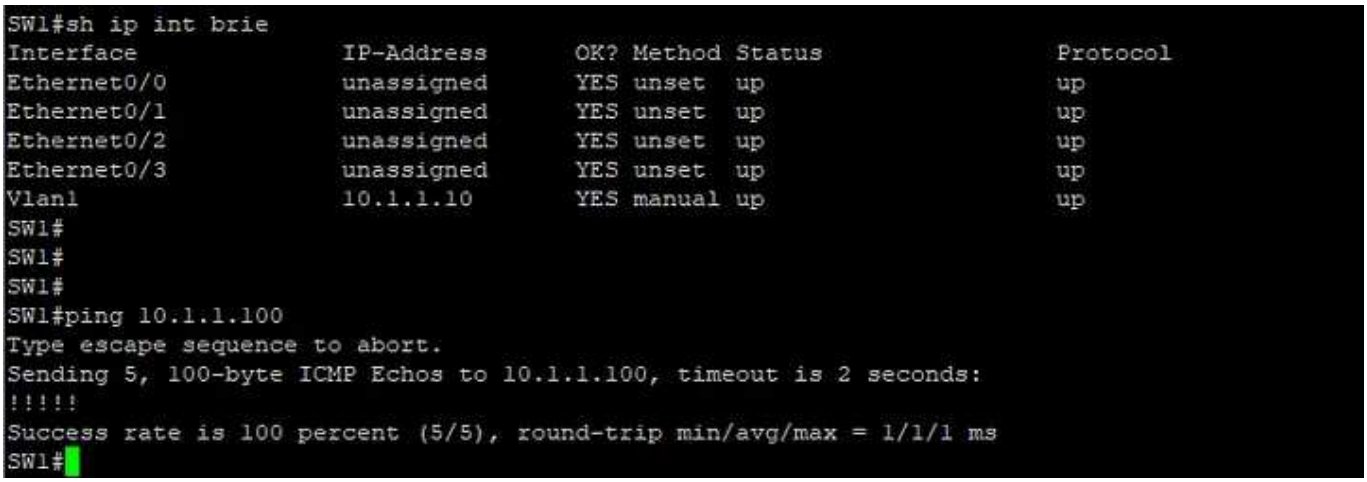


A única diferença, é que eu criei um grupo para nosso **NAD** (apenas para organização), chamado Switches, repare na figura acima.

A topologia do nosso lab ficou assim (adicionei mais um cliente para o 802.1x):



Acessando o switch, veja as configurações simples de IP e teste básico de conectividade.



Pronto, agora vamos lá, os passos para a configuração do servidor **radius** e de **autenticação** no switch:

1) Habilitar o AAA

```
aaa new-model
```

2) Criação do servidor radius

```
aaa group server radius ISE
 server name ISE
radius server ISE
 address ipv4 10.1.1.100 auth 1812 acc 1813
 key cisco
```

3) Vamos proteger o acesso via console (quem nunca ficou preso “pra fora” do equipamento? :P)

```
aaa authentication login NOAUTH none
line con 0
 login authen NOAUTH
```

4) Vamos habilitar a **autenticação, autorização e accounting** via Dot1x e MAB — sempre apontando para o grupo 'ISE' que criamos no passo 2

```
aaa authentication dot1x default group ISE
aaa authorization network default group ISE
aaa accounting dot1x default start-stop group ISE
```

5) Habilitar o *ip device tracking* e o Dot1x no switch

```
ip device tracking
dot1x system-auth
```

6) Agora faremos configuração da porta e0/1, onde está o cliente MAB

```
interface ethernet0/1
 switchport mode access
 dot1x pae authenticator
 mab
 authentication order mab dot1x
 authentication priority dot1x mab
 authentication port-control auto
```

7) E finalmente a configuração da porta e0/2, onde está o cliente Dot1x (idem acima, pois ambas estão habilitadas MAB e Dot1x)

```
interface ethernet0/2
 switchport mode access
 dot1x pae authenticator
 mab
 authentication order mab dot1x
 authentication priority dot1x mab
 authentication port-control auto
```

Como última *task*, vamos rapidinho criar um **DHCP Server** no switch:

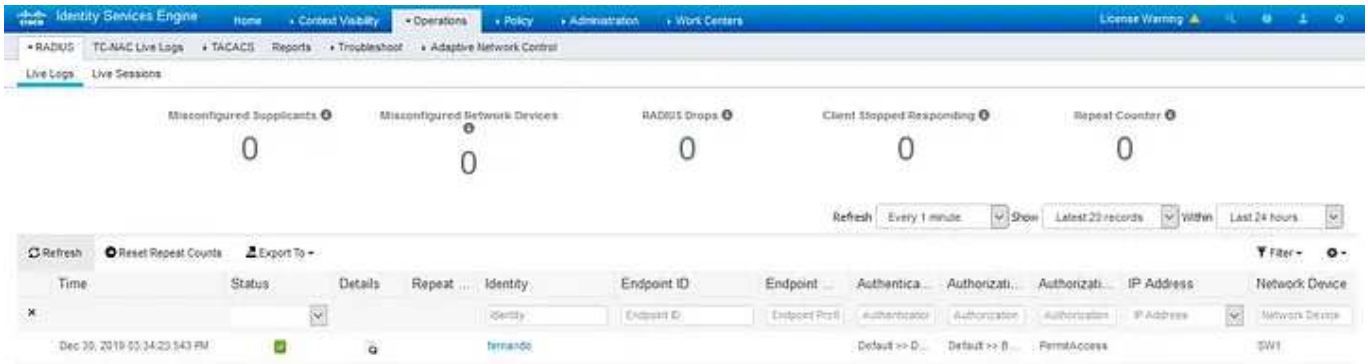
```
ip dhcp excluded-address 10.1.1.1
!IP do meu notebook
ip dhcp excluded-address 10.1.1.10
!IP do switch
ip dhcp excluded-address 10.1.1.100
!IP do ISE

ip dhcp pool VLAN1
 network 10.1.1.0 /24
 default-router 10.1.1.10
 dns-server 10.1.1.10
```

Nesse momento, eu costumo fazer um teste simples de autenticação, veja abaixo:

```
SW1#test aaa group ISE fernando Cisco123! legacy
Attempting authentication test to server-group ISE using radius
User was successfully authenticated.
```

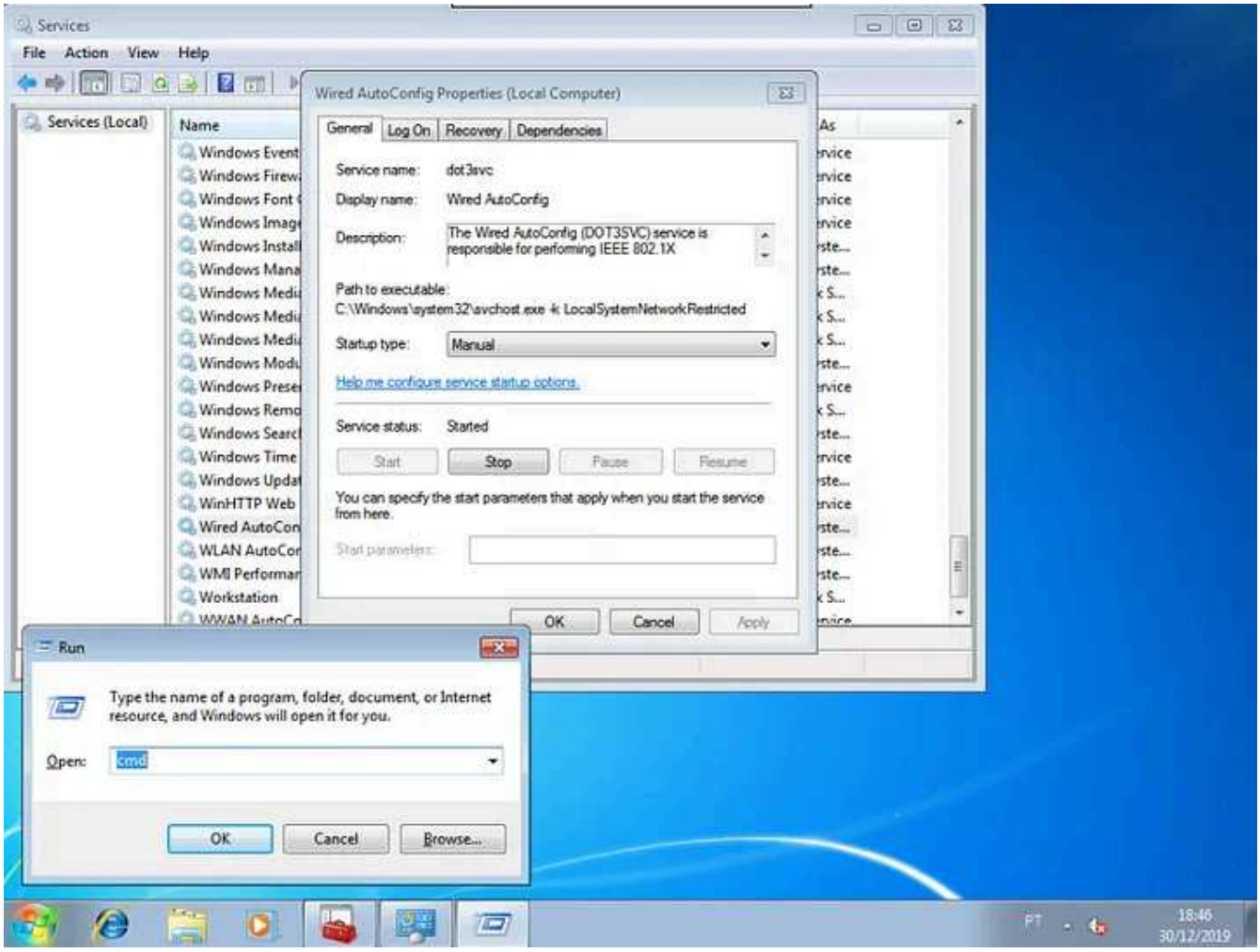
Esse usuário fernando, nós criamos no artigo anterior (ISE Basics — Parte 2)

Aqui, os logs do ISE em *Operations* > *RADIUS* > *Live Logs:*



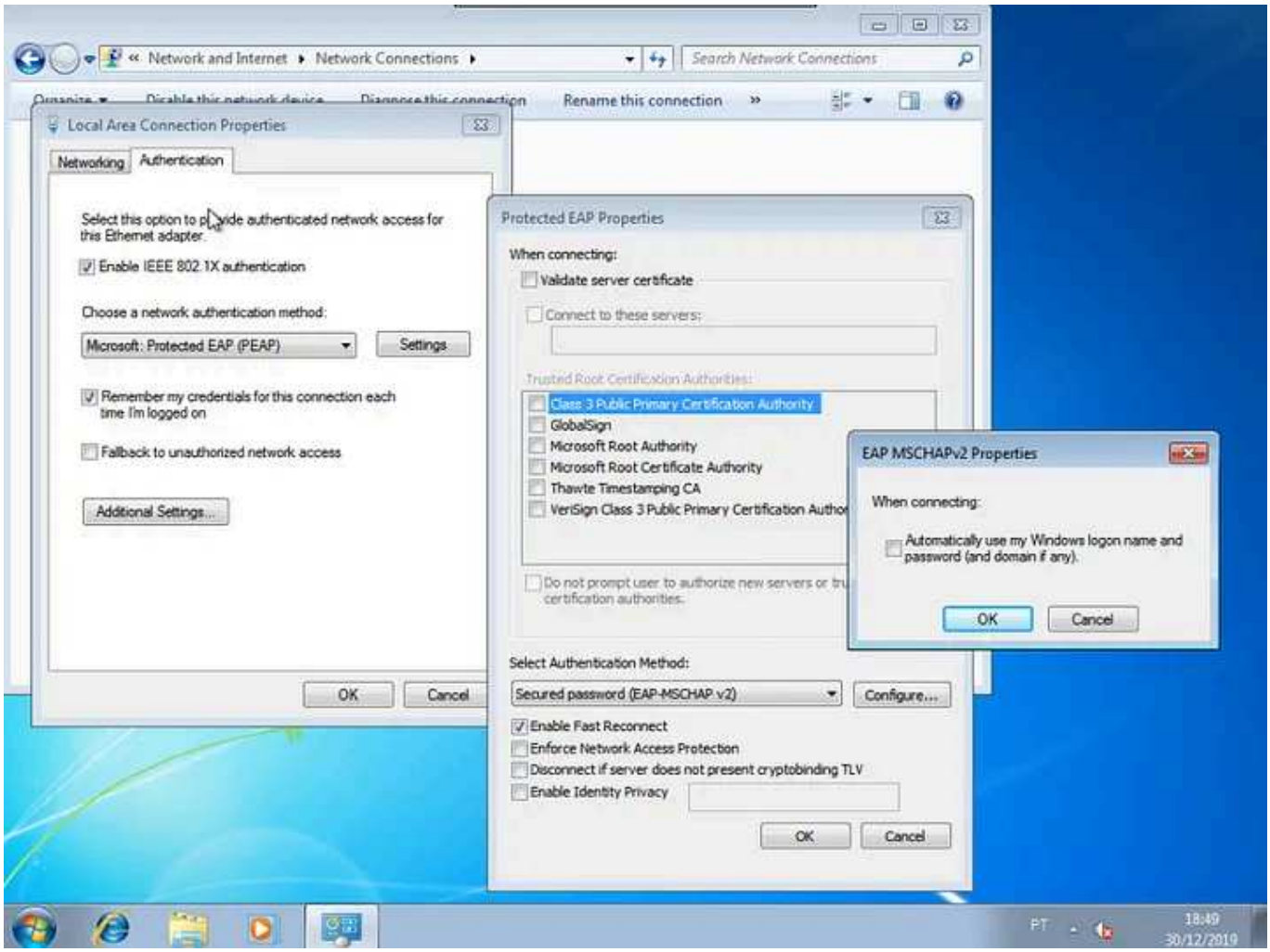
Começando então pelo cliente do 802.1X, já que o usuário já está criado e OK.

Acessando a máquina Windows, vamos confirmar que o serviço *WiredAutoConfig*, que habilita o 802.1X na LAN está rodando. Em caso negativo, inicie ele:

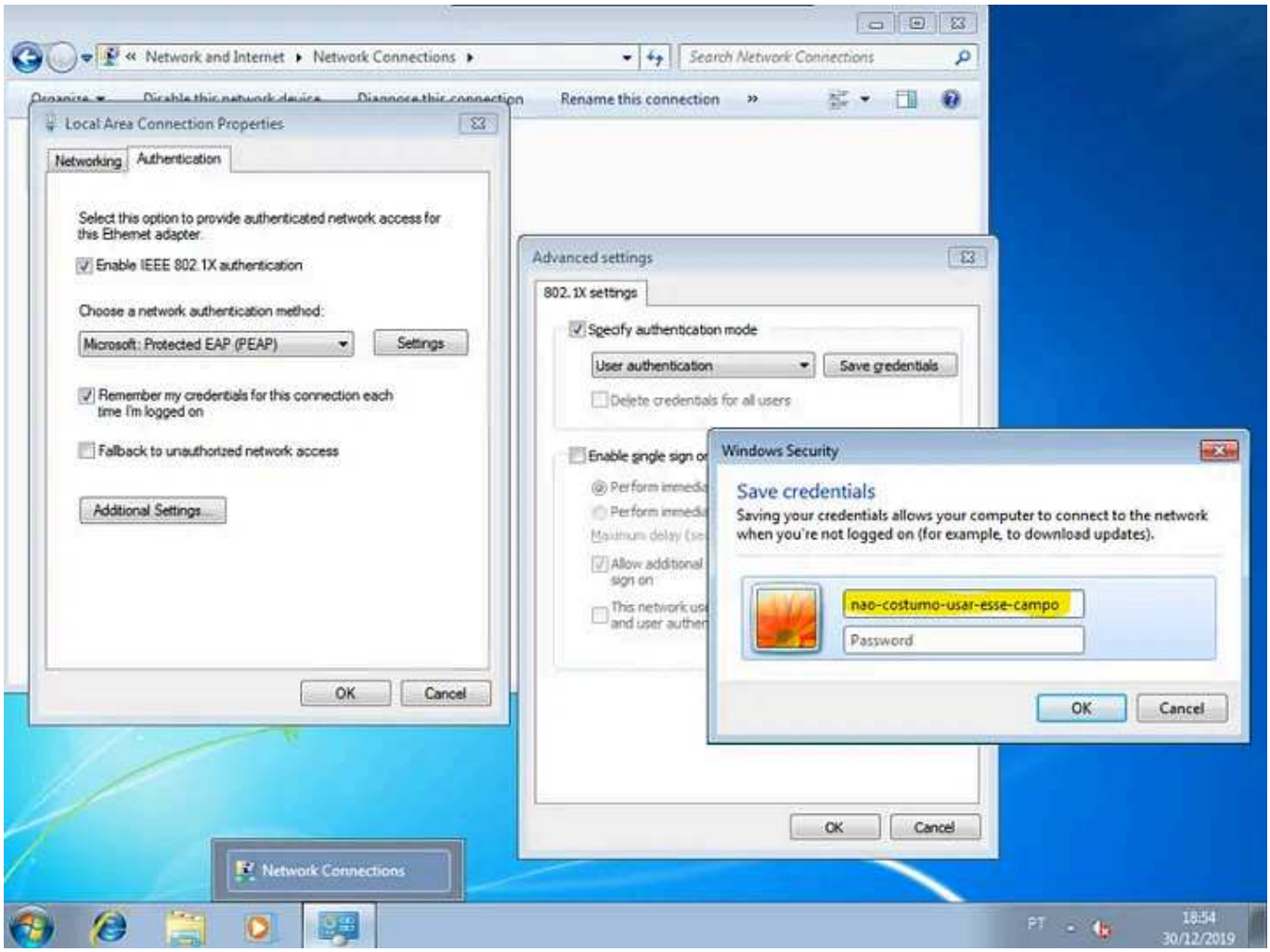


Agora a configuração da placa de rede. Clicar com o botão direto, propriedades e aba *Authentication*:

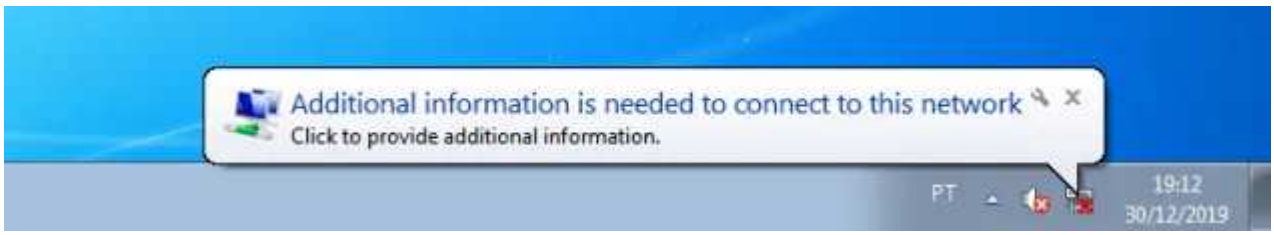
Selecione **PEAP** e depois em configurações, desmarque para validar o certificado do servidor (já que não estamos usando certificado digital nesse caso) e, em configuração do método de autenticação, desmarque para usarmos o usuário do Windows.



Dê OK em tudo e em configurações adicionais, deixe marcado para autenticação de usuário — aqui eu costumo deixar
sem *user* e *password* pré-definidos, mas você pode configurar se preferir.



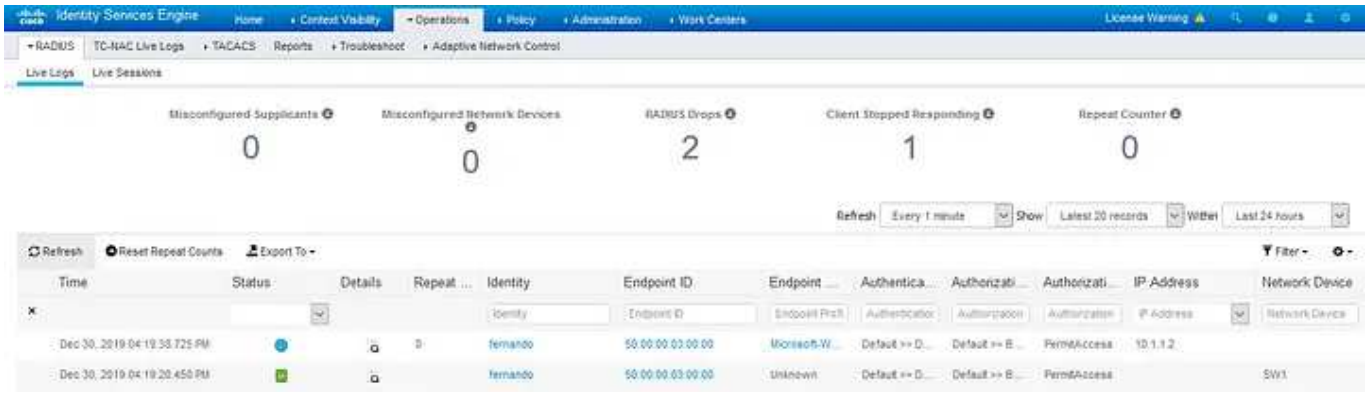
E, finalmente, estamos prontos para o teste. A porta do switch estava em *shutdown*, alterei ela, e apareceu um balão no Windows pedindo usuário e senha (caso não aconteça, desabilite e habilite o adaptador de rede):



Clique nele e entre com usuário fernando, que criamos no post anterior e testamos no switch no início do artigo.

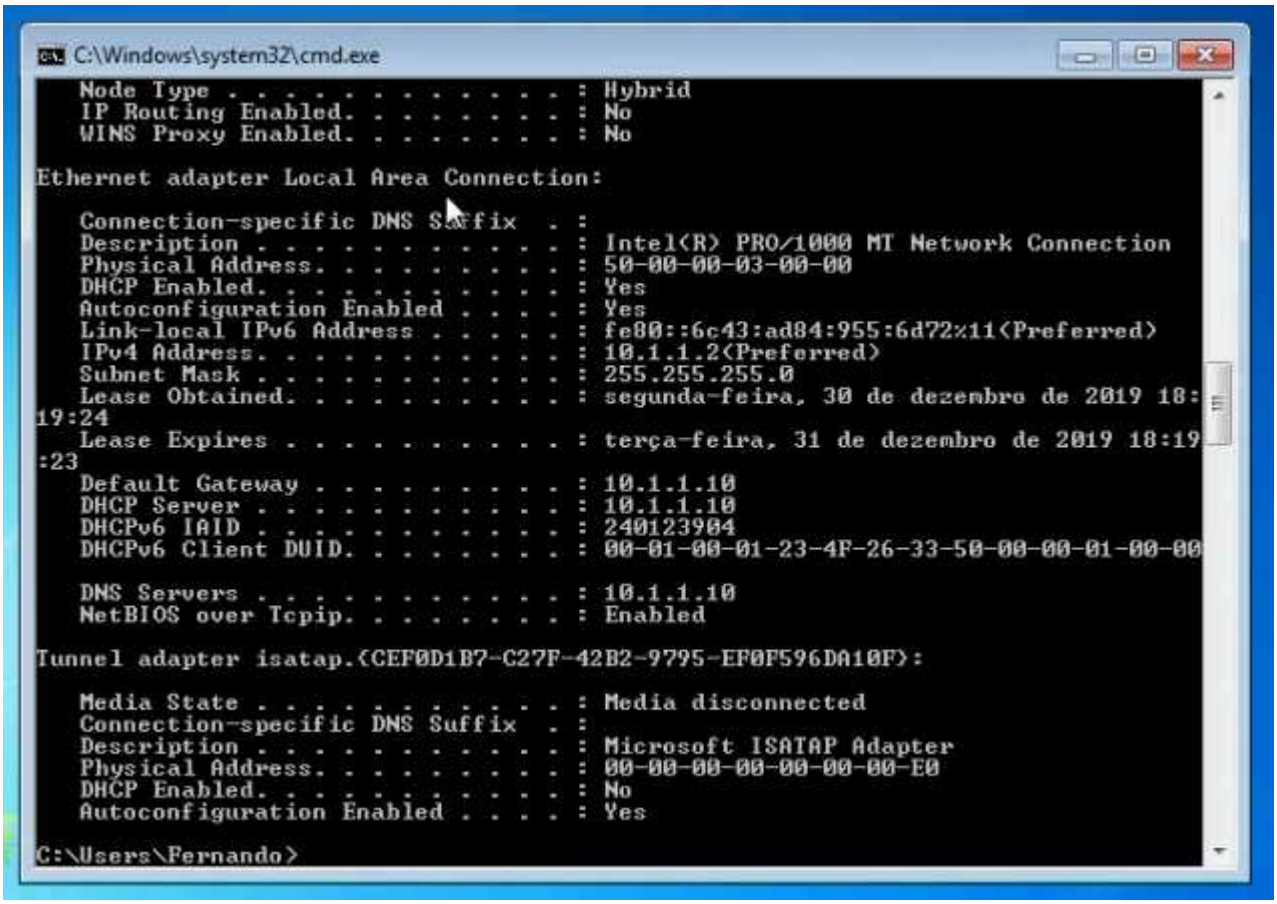
Repare agora nas telas que confirmam a autenticação bem sucedida.

Logs do ISE em *Operations* > *RADIUS* > *Live Logs*



Obs: São duas entradas pois a de baixo é a autenticação em si, e a de cima, a **sessão** RADIUS que foi criada.

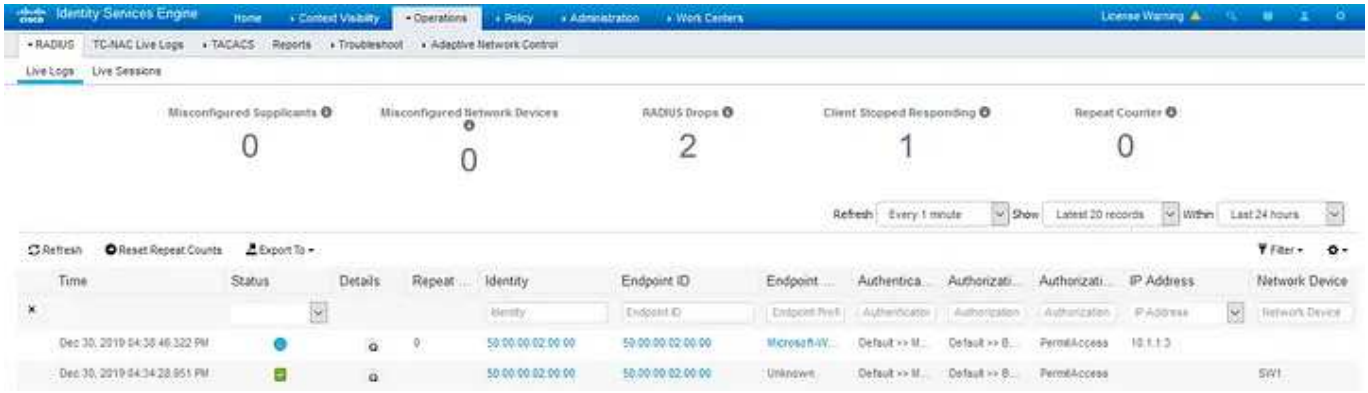
E nosso cliente se autenticou e já pegou IP:



Dê um 'show authentication sessions' no switch e você verá a autenticação e autorização bem sucedida. Repare no método:

```
SW1#sh authe sessions

Interface    Identifier     Method  Domain  Status Fg Session ID
Et0/2        5000.0003.0000 dot1x   DATA    Auth
0A01010A00000013004B82AB

Session count = 1

Key to Session Events Blocked Status Flags:

A - Applying Policy (multi-line status for details)
  D - Awaiting Deletion
  F - Final Removal in progress
  I - Awaiting IIF ID allocation
  N - Waiting for AAA to come up
  P - Pushed Session
  R - Removing User Profile (multi-line status for details)
  U - Applying User Profile (multi-line status for details)
  X - Unknown Blocker
```

Vamos agora ligar a máquina Windows que irá se autenticar com **MAB**. Nesse caso, não é necessário nenhuma configuração no cliente. Nos logs do ISE, agora vemos um MAC Address ao invés de um usuário.



No switch, temos agora duas portas autenticadas. A primeira é a do MAB e a segunda do 802.1X. Repare no método em destaque:

```
SW1#show authentication sessions

Interface    Identifier     Method  Domain  Status Fg Session ID
Et0/1        5000.0002.0000 mab     DATA    Auth
0A01010A0000001400585EC1
```

```
Et0/2        5000.0003.0000 dot1x   DATA    Auth
0A01010A00000013004B82AB

Session count = 2

Key to Session Events Blocked Status Flags:

A - Applying Policy (multi-line status for details)
  D - Awaiting Deletion
  F - Final Removal in progress
  I - Awaiting IIF ID allocation
  N - Waiting for AAA to come up
  P - Pushed Session
  R - Removing User Profile (multi-line status for details)
  U - Applying User Profile (multi-line status for details)
  X - Unknown Blocker
```

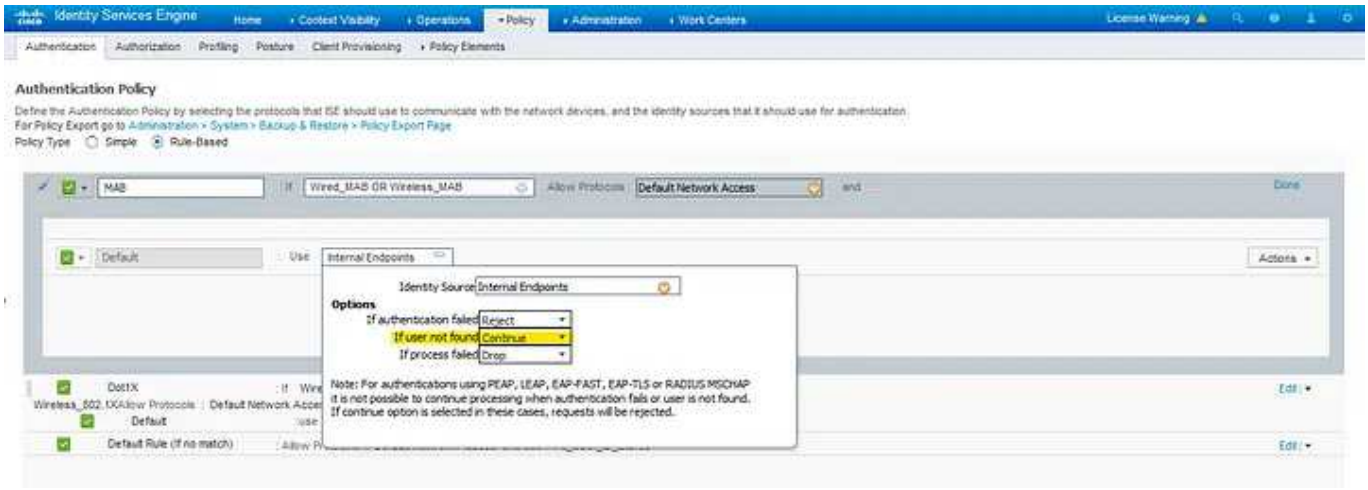
O Windows também pegou um IP, assim como a primeira máquina:

```
SW1#show ip dhcp binding
Bindings from all pools not associated with VRF:
IP address      Client-ID/              Lease expiration
Type       State      Interface
               Hardware address/
               User name
10.1.1.2         0150.0000.0300.00       Dec 31 2019 08:19 PM
Automatic  Active     Vlan1
10.1.1.3         0150.0000.0200.00       Dec 31 2019 08:38 PM
Automatic  Active     Vlan1
```

E, por fim, tráfego liberado entre as máquinas.

```
SW1#ping 10.1.1.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.1.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/3
ms
SW1#ping 10.1.1.3
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.1.3, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/2
ms
```

> ***Obs**: Você deve ter reparado que no caso do cliente Dot1x nós criamos um usuário, mas não criamos um **endpoint** para o cliente MAB. Isso porque por padrão na versão 2.1, o ISE mesmo que não exista um endpoint, ele permite que o processo continue. Essa configuração é feita aqui:*

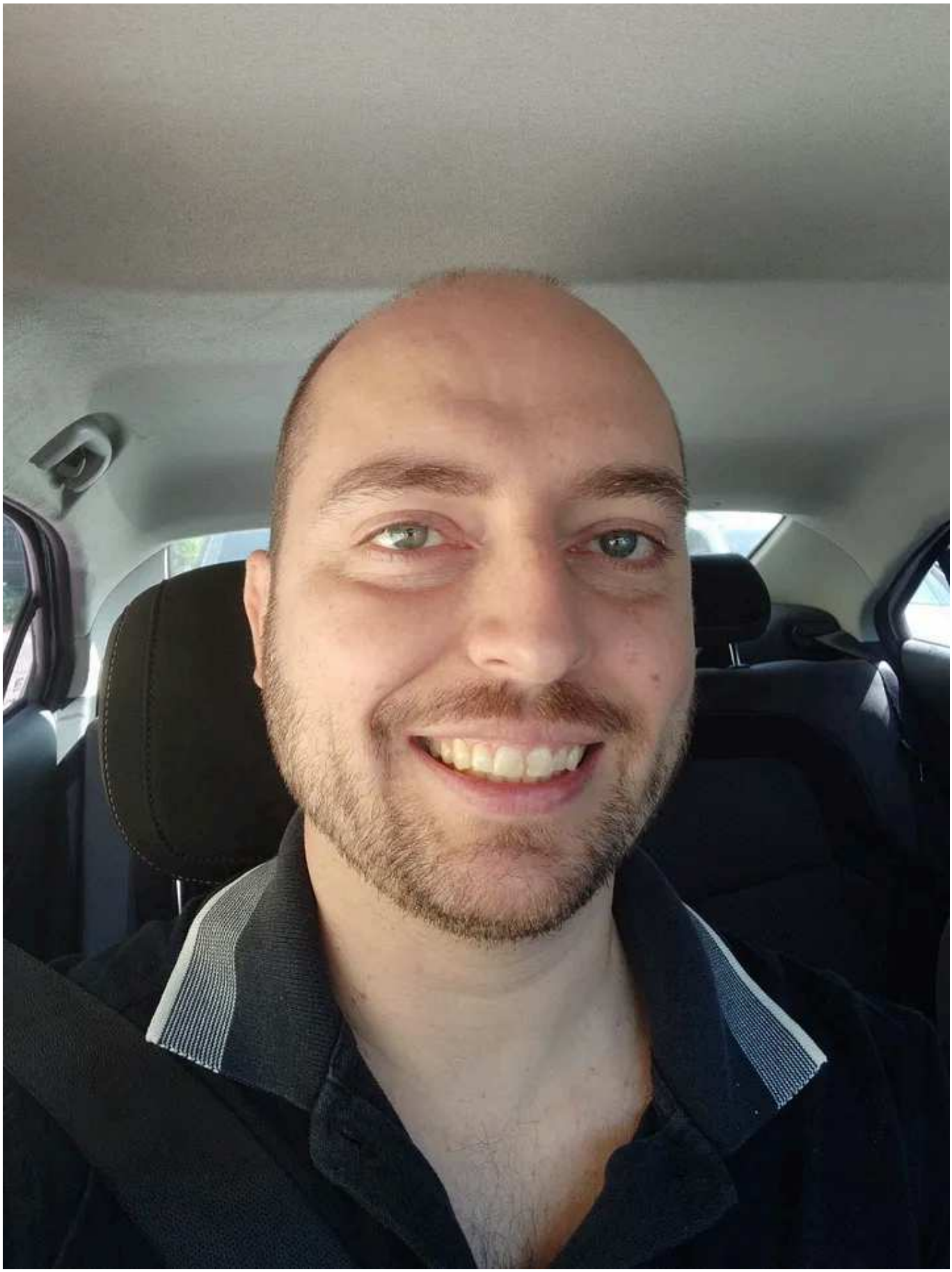


Nos próximos artigos iremos testar configurações de política de autenticação e autorização diferentes.

Abraços!!

Se você gostou, deixa seu **“claps”** aí do lado esquerdo e **compartilhe** nos seus grupos. Você também pode me seguir e a TechRebels!

Sobre o autor:



Fernando Mantovani Pierobon trabalha há **18 anos** na área de TI sendo 14 com segurança da tecnologia da informação.

É formado em **Ciências da Computação** e **CCIE Security #63268**.

https://www.linkedin.com/in/fernandomantovani/

Dot1x Mab Security Cybersecurity Cisco