**[Windows HELL](https://windowshell.wordpress.com/" \o "Windows HELL) (No final tem o artigo traduzido)**

Dante was wrong, the first circle of hell isn't limbo… it's Windows!

https://windowshell.wordpress.com/2011/01/04/a-sample-802-1x-configuration-guide/

**A sample 802.1X configuration guide**

Due to the complexity of 802.1X configuration, there is a lot of documentation out there. Unfortunately, due to the complexity of 802.1X, there are very few step-by-step guides on actually setting a system up to use it. This is merely a crib sheet that I use to create a nominal 802.1X configuration. This setup uses computer certificates only, with users logging in with passwords (not smart cards). The servers are Enterprise 2008 R2, and the clients are Windows XP SP3 and Windows 7.  Network gear consisted of Cisco 3750 and 2960 switches running IOS 12.2(52).  **Note that you have to have a K9 version of the IOS, otherwise the security features are not available**.  These instructions may or may not work if you are on different server/client versions.  I know there are NPS client limitations on the Standard server version and that you cannot create custom certificates on Standard either.  So Enterprise or better is required for your servers.  Hopefully, someone out there will find this helpful. As there are many, many, many ways to configure this stuff, you may need to adjust it for your needs. I cannot profess that I am an expert by any means, but if you have a question about something in (or not in) this checklist, please leave a comment.

Configuration of 802.1X is a multi-step process. Reference: <http://technet.microsoft.com/en-us/library/cc753354(WS.10).aspx>. Intel vPro AMT, if used, should be configured and operational prior to running this procedure.

1. Certificate Services  
   This procedure assumes that an Enterprise CA has been previously installed and that client certificates have been provisioned to all workstations in the enterprise via Group Policy. Additionally, your primary site servers have been added into an AD security group called ‘SCCM Primary Site Servers’
   1. In this step, we will create and deploy the NPS certificate template.
      1. On the certification authority server, start the Certification Authority MMC snap-in
      2. Expand the CA node.
      3. In the console tree, right-click Certificate Templates. Select the Manage option. The Certificate Templates console will appear. Note the Domain Controller that the Console is connected to.
      4. In the details pane, click the RAS and IAS Server template.
      5. On the Action menu, click Duplicate Template. In the Duplicate Template dialog box, select the Windows Server 2003, Enterprise Edition template version.
      6. Click OK. The Properties dialog box for the certificate template opens.
      7. On the General tab, in Display Name, type a name for the new certificate template.
      8. Click the Security tab. In Group or user names, click RAS and IAS servers.
      9. In Permissions for RAS and IAS servers, under Allow, select the Enroll and Autoenroll permission check boxes, and then click OK.
      10. Close the Certificate Templates Console.
      11. Force replication across Domain Controllers using Active Directory Sites and Services. Begin replication from the server noted earlier.
      12. In the Certification Authority Console, right-click the Certificate Templates node. On the Action menu, point to New, and then click Certificate Template to Issue.
      13. Select the template that was just created, and then click OK.
   2. (If using Intel AMT, otherwise go to next section). Here, we will create the Client Authentication certificates for 802.1X AMT-Based computers. This is separate from the normal client certificates issued by the domain.
      1. In the console tree, right-click Certificate Templates. Select the Manage option. The Certificate Templates console will appear. Note the Domain Controller that the Console is connected to.
      2. In the details pane, right-click the entry that displays Workstation Authentication in the column Template Display Name, and then click Duplicate Template. In the Duplicate Template dialog box, select the Windows Server 2003, Enterprise Edition template version.
      3. Click OK. The Properties dialog box for the certificate template opens.
      4. On the General tab, in Display Name, type a name like ‘AMT 802.1X Client Authentication’.
      5. Click the Subject Name tab, and then click Supply in the request. Click OK in the warning dialog box for this setting.
      6. Click the Security tab, and remove the Enroll permission from the security groups Domain Admins and Enterprise Admins.
      7. Click Add, and add SCCM Primary Site Servers.
      8. Select the following Allow permissions for this group: Read and Enroll.
      9. Close the Certificate Templates Console.
      10. Force replication across Domain Controllers using Active Directory Sites and Services. Begin replication from the server noted earlier.
      11. In the Certification Authority Console, right-click the Certificate Templates node. On the Action menu, point to New, and then click Certificate Template to Issue.
      12. Click AMT client template, and then click OK.
2. NPS server
   1. Ensure that the NPS server is a member of the ‘RAS and IAS Server’ group in Active Directory.
   2. Restart the server so it can autoenroll the newly assigned server certificate. If the certificate does not autoenroll, open a Certificates MMC session on the server and manually enroll the machine.
   3. Open the Server Manager Console and expand the tree to Roles | Network Policy and Access Services | NPS (local) | Policies | Connection Request Policies. Create a new Connection Request Policy. Name the new policy ‘Secure (Wired) Ethernet Connections’. Leave the type of network access server as Unspecified. Click Next.
   4. Add a new condition: NAS Port Type. In the popup, under Common 802.1X connection tunnel types, select Ethernet. Click OK, then Next.
   5. On the Specifiy Connection Request Forwarding, ensure ‘Authenticate requests on this server’ is ticked and click Next.
   6. Continue clicking Next until the Finish option appears, then click Finish.
   7. Verify the new policy is enabled and listed as Processing Order 1.
   8. In the tree, select ‘Network Policies’ and create a new network policy name ‘Secure Wired (Ethernet) Connections’.
   9. Type of network access server is ‘Unspecified’.
   10. Under Conditions, set ‘NAS Port Type’ to ‘Ethernet’, and ‘Windows Groups’ to ‘Domain Computers’ and ‘Domain Users’. Note that the ‘Windows Groups’ criteria should be a logical OR.
   11. Access permission is ‘Granted’.
   12. Add EAP Type ‘Microsoft: Protected EAP (PEAP). Verify the settings have a certificate association, ‘Enable Fast Reconnect’, and EAP subtype of ‘Secured password (EAP-MSCHAP v2).
   13. Leave the default ‘Less secure authentication methods’ as is.
   14. Do not configure any constraints
   15. Add the following Standard attributes (if you want to pass VLAN settings via the NPS server):
       1. Tunnel-Medium-Type: 802
       2. Tunnel-Preference: 1
       3. Tunnel-Pvt-Group-ID: <ID number or name of VLAN>
       4. Tunnel-Type: VLAN
   16. Set the newly created policy at Processing Order 1.
3. SCCM configuration (If using Intel AMT, otherwise go to next section)
   1. In the Configuration Manager console, navigate to System CenterConfiguration Manager / Site Database / Site Management / <site code> – <site name> / Site Settings / Component Configuration.
   2. Right-click Out of Band Management, click Properties, and then click the 802.1X and Wireless tab.
   3. To configure 802.1X authentication for wired networks, select Enable 802.1X authentication for wired network access, and then click Set.
   4. In the Trusted Root Certificate for RADIUS Authentication dialog box, specify the trusted root certificate by selecting an enterprise CA from the forest. Ensure that From certification authority (CA) is selected, and select the CA from the drop-down list.
   5. Use the drop-down box to select PEAPv0/EAP-MSCHAPv2 as the client authentication method.
   6. Click Use client certificate to use a client certificate for authentication.
   7. Click Select, specify the Issuing CA to use for the client certificate and the RADIUS client certificate template ‘AMT 802.1X Client Authentication’, and then click OK.
   8. On ‘Out of Band Management Properties’ window, click OK.
4. Group Policy  
   CAUTION: DUE TO A BUG IN WINDOWS 2008 R2/WINDOWS 7, THIS GPO MUST BE CREATED ON A WINDOWS 2008 RTM MACHINE. OTHERWISE, THE GPO WILL NOT APPLY PROPERLY AND YOU WILL GET A CONNECTION FAILURE ERROR DUE TO ‘VALIDATE SERVER CERTIFICATE’ BEING ERRONEOUSLY CHECKED. See<http://blogs.technet.com/b/asiasupp/archive/2010/11/03/validate-server-certificate-option-is-unexpected-to-check-in-wired-network-ieee-802-3-policies.aspx>
   1. Create a new group policy
      1. Computer Configuration | Policies | Windows Settings | Security Settings | System Services. Define ‘Wired AutoConfig’ to Automatic with default security.
      2. Computer Configuration | Policies | Windows Settings | Security Settings | Wired Network (IEEE 802.3) Policies. Create a new wired network policy.
         1. Name the policy
         2. Ensure ‘Use Windows Wired Auto Config service for clients’ is checked.
         3. On the Security tab:
            1. ‘Enable use of IEEE 802.1X authentication for network access’ is checked.
            2. Network authentication method is ‘Microsoft: Protected EAP (PEAP)’.
            3. Click ‘Properties’:

Uncheck ‘Validate server certificate’

Authentication method is ‘Secured Password (EAP-MSCHAP v2)’.

Click ‘Configure…’. Ensure Windows logon option is checked.

‘Enable Fast Reconnect’ is checked.

Close ‘Protected EAP Properties’ window.

* + - * 1. Authentication Mode is ‘User re-authentication’.
        2. ‘Cache user information for subsequent connection to this network’ is checked.
        3. Click ‘Advanced…’:

‘Enable Single Sign On for the network’ is checked.

‘Allow additional dialogs to be displayed during Single Sign On’ is unchecked.

Close ‘Advanced security settings’ window.

* + - 1. Close policy properties window.

1. Network Devices  
   NOTE: This configuration assumes that RADIUS is already configured for on the switch for other uses (i.e. SSH logins). If not, you’ll need to create an association in the NPS server and input the server address and shared secret on the device configuration. Chuck Murison has a great blog on how to do this at: <http://murison.wordpress.com/2010/11/11/cisco-radius-configuration-with-server-2008-r2/>
   1. Enable RADIUS for 802.1X (at the global configuration prompt)
      1. aaa authentication dot1x default group radius  
         This sets the device to use RADIUS for 802.1X authentication
      2. aaa authorization network default group radius  
         This sets the device to use RADIUS to authorize users for specific access
      3. authentication mac-move permit  
         This allows machines to be moved while a session is open (device closes old session)
      4. dot1x system-auth-control  
         Globally turns on 802.1X authentication
   2. On a PER PORT basis, issue the following commands (a range command may be used to configure ports simultaneously):
      1. mab  
         This allows for MAC authentication bypass (where required)
      2. authentication order dot1x mab  
         This tells the network device to use 802.1X before MAB
      3. authentication priority dot1x mab  
         This tells the network device to prioritize 802.1X before MAB
      4. dot1x pae authenticator  
         This prevents the downline client from trying to be a supplicant
      5. authentication port-control auto  
         This turns on 802.1X for the port.
      6. Port may need to be shut/no shut to force the client to authenticate.
   3. Follow-on actions
      1. Set the default VLAN for the port to something else (i.e. a guest or offline vlan). The VLAN is automatically switched to the operations VLAN once authenticated.
      2. Set a guest vlan for machines that are being imaged and not yet capable of 802.1X authentication. On the interface:  
         dot1x guest-vlan <vlan-id>
      3. Device settings may need to be adjusted to prevent DHCP timeout prior to 802.1X timeout. The following settings were successfully used in the test lab:
         1. dot1x timeout quiet-period 3  
            This setting is the idle time between failed authentication and the next attempt.
         2. dot1x timeout tx-period 5  
            This setting is the idle time between transmissions.

***TRADUÇÃO:***

# [janelas HELL](https://windowshell.wordpress.com/)

Dante estava errado, o primeiro círculo do inferno não limbo é ... é o Windows!

[Ir para o conteúdo](https://windowshell.wordpress.com/2011/01/04/a-sample-802-1x-configuration-guide/#content)

* [Sobre](https://windowshell.wordpress.com/about/)

[« Status Monitor McAfee Agent em x64 / Sistemas Server Core](https://windowshell.wordpress.com/2010/11/12/mcafee-agent-status-monitor-on-x64server-core-systems/)

[Internet Explorer suga »](https://windowshell.wordpress.com/2011/01/26/internet-explorer-sucks/)

## Um guia configuração 802.1X amostra

Devido à complexidade da configuração 802.1X, há uma grande quantidade de documentação lá fora. Infelizmente, devido à complexidade do 802.1X, há muito poucos guias passo-a-passo sobre realmente a criação de um sistema para usá-lo. Esta é apenas uma folha de berço que eu uso para criar uma configuração nominal 802.1X. Esta configuração utiliza certificados de computador, apenas com usuários entrando com senhas (não cartões inteligentes). Os servidores estão Empresa 2008 R2, e os clientes são o Windows XP SP3 e Windows 7. equipamentos de rede Cisco consistia em 3750 e 2960 muda rodando IOS 12.2 (52).  **Note-se que você tem que ter uma versão K9 do IOS, caso contrário, a segurança recursos não estão disponíveis** . Essas instruções podem ou não podem trabalhar se você estiver em diferentes versões servidor / cliente. Sei que existem limitações cliente NPS na versão padrão do servidor e que você não pode criar certificados personalizados em padrão também. Assim Empresa ou melhor é necessário para seus servidores. Felizmente, alguém lá fora vai achar isso útil. Como existem muitas, muitas, muitas maneiras de configurar este material, pode ser necessário ajustá-lo às suas necessidades.Eu não pode professar que eu sou um especialista, por qualquer meio, mas se você tiver uma pergunta sobre algo (ou não em) esta lista, por favor deixe um comentário.

Configuração de 802.1x é um processo multi-passo. Referência: <http://technet.microsoft.com/en-us/library/cc753354(WS.10).aspx> . Intel vPro AMT, se utilizado, deve ser configurado e antes operacional para executar este procedimento.

1. Serviços de Certificados   
   Este procedimento pressupõe que um Enterprise CA tenha sido previamente instalado e que os certificados de cliente têm sido fornecidos para todas as estações de trabalho na empresa por meio da Diretiva de Grupo. Além disso, os servidores de site primários foram adicionados a um grupo de segurança AD chamado "Servidores SCCM primária no site '
   1. Nesta etapa, vamos criar e implantar o modelo de certificado NPS.
      1. No servidor de autoridade de certificação, iniciar o MMC Autoridade de Certificação snap-in
      2. Expanda o nó CA.
      3. Na árvore da consola, clique com o botão direito em Modelos de certificado. Selecione a opção Gerenciar. O console de Modelos de Certificado aparecerá. Observe o controlador de domínio que a consola está ligada a.
      4. No painel de detalhes, clique no modelo de RAS e IAS Server.
      5. No menu ação, clique em Duplicar modelo. Na caixa de diálogo Modelo Duplicado, selecione o Windows Server 2003, Enterprise Edition versão do modelo.
      6. Clique em OK. A caixa de diálogo Propriedades para o modelo de certificado é aberto.
      7. Na guia Geral, em Nome de exibição, digite um nome para o novo modelo de certificado.
      8. Clique na guia Segurança. Em Nomes de grupo ou de usuário, clique servidores RAS e IAS.
      9. Em Permissões para Servidores RAS e IAS, em Permitir, marque as caixas de seleção de permissão Registrar e Registrar automaticamente e clique em OK.
      10. Feche o Console Modelos de certificado.
      11. Forçar a replicação entre controladores de domínio usando Serviços e sites do Active Directory. Comece a replicação do servidor mencionado anteriormente.
      12. No Certification Authority Console, clique com o botão direito no nó Modelos de Certificado. No menu ação, aponte para novo e, em seguida, clique em Modelo de certificado a ser emitido.
      13. Selecione o modelo que acabou de ser criada e clique em OK.
   2. (Se estiver usando Intel AMT, caso contrário, ir para a próxima seção). Aqui, vamos criar os certificados de autenticação de cliente para computadores 802.1X AMT-based. Esta é separado dos certificados de cliente normais emitidos pelo domínio.
      1. Na árvore da consola, clique com o botão direito em Modelos de certificado. Selecione a opção Gerenciar. O console de Modelos de Certificado aparecerá. Observe o controlador de domínio que a consola está ligada a.
      2. No painel de detalhes, clique com botão direito na entrada que exibe Authentication Workstation no modelo coluna Display Name e clique em Duplicar modelo. Na caixa de diálogo Modelo Duplicado, selecione o Windows Server 2003, Enterprise Edition versão do modelo.
      3. Clique em OK. A caixa de diálogo Propriedades para o modelo de certificado é aberto.
      4. Na guia Geral, em Nome de exibição, digite um nome como 'AMT 802.1X autenticação de cliente'.
      5. Clique na guia Nome do assunto, e depois clique de alimentação no pedido. Clique em OK na caixa de diálogo de aviso para esta definição.
      6. Clique na guia Segurança, e retire a permissão Inscrever dos grupos de segurança Administradores de Domínio e Administradores de Empresa.
      7. Clique em Adicionar e adicionar servidores SCCM site principal.
      8. Selecione as seguintes Permitir que as permissões para este grupo: leitura e registro.
      9. Feche o Console Modelos de certificado.
      10. Forçar a replicação entre controladores de domínio usando Serviços e sites do Active Directory. Comece a replicação do servidor mencionado anteriormente.
      11. No Certification Authority Console, clique com o botão direito no nó Modelos de Certificado. No menu ação, aponte para novo e, em seguida, clique em Modelo de certificado a ser emitido.
      12. Clique modelo de cliente AMT e clique em OK.
2. servidor NPS
   1. Verifique se o servidor NPS é membro dos "RAS e IAS Servidor 'grupo no Active Directory.
   2. Reinicie o servidor para que ele possa registrar automaticamente o certificado de servidor recém-atribuído. Se o certificado não registrar automaticamente, abra uma sessão MMC Certificados no servidor e registrar manualmente a máquina.
   3. Abra o Console Server Manager e expanda a árvore para Roles | Política de Rede e Serviços de Acesso | NPS (local) | políticas | Pedido de Ligação Políticas. Criar uma nova política de pedido de ligação. Nomeie a nova política 'seguros (com fio) conexões Ethernet'. Deixar o tipo de servidor de acesso de rede como não especificado. Clique em Avançar.
   4. Adicionar uma nova condição: NAS Port Type. No pop-up, sob 802.1X Comum túnel tipos de conexão, selecione Ethernet. Clique em OK, em seguida, em Avançar.
   5. Na especificar Connection Request Forwarding, assegurar «autenticar solicitações neste servidor 'está marcada e clique em Avançar.
   6. Continue a clicar em Avançar até a opção Finish aparecer, clique em Concluir.
   7. Verifique a nova política é ativado e listado como Processamento de Ordem 1.
   8. Na árvore, selecione "Políticas de Rede 'e criar um nome de política nova rede' Fixe Wired Connections (Ethernet)".
   9. Tipo de servidor de acesso à rede é «indeterminado».
   10. Sob condições, definir 'NAS Port Type' para 'Ethernet' e 'Grupos do Windows' para 'Computadores do domínio' e 'Domain Users'. Note-se que os critérios dos grupos do Windows deve ser uma lógica OR.
   11. permissão de acesso é "Concedido".
   12. Adicionar EAP Type 'Microsoft: EAP Protegido (PEAP). Verifique as configurações de ter uma associação certificado, 'Ativar reconexão rápida', e EAP subtipo de 'password segura (EAP-MSCHAP v2).
   13. Deixe 'métodos de autenticação menos seguros "o padrão como é.
   14. Não configure quaisquer restrições
   15. Adicione os seguintes atributos padrão (se você quer passar configurações de VLAN através do servidor NPS):
       1. Tunnel-Medium-Type: 802
       2. Tunnel-Preference: 1
       3. Tunnel-Pvt-Group-ID: <número de identificação ou nome da VLAN>
       4. Tunnel-Type: VLAN
   16. Definir a política recém-criada na Ordem de Processamento 1.
3. configuração do SCCM (Se ​​estiver usando Intel AMT, caso contrário, vá para a próxima seção)
   1. No console do Configuration Manager, navegue até Sistema CenterConfiguration Gerente / site de banco de dados / Gestão Site / <código do site> - Definições <nome do site> / Site / Configuração de componentes.
   2. Botão direito do mouse Out of Band Management, clique em Propriedades e clique na guia 802.1X e sem fio.
   3. Para configurar a autenticação 802.1X para redes com fio, selecione Ativar a autenticação 802.1X para acesso à rede com fio, e, em seguida, clique em Definir.
   4. No certificado de raiz fidedigna caixa de diálogo Autenticação RADIUS, especifique o certificado raiz confiável, selecionando uma AC empresarial da floresta. Certifique-se de que a partir de autoridade de certificação (CA) é selecionado, e selecione a CA a partir da lista drop-down.
   5. Use a caixa de drop-down para selecionar PEAPv0 / EAP-MSCHAPv2 como o método de autenticação do cliente.
   6. Clique em Usar certificado de cliente para usar um certificado de cliente para autenticação.
   7. Clique em Selecionar, especifique o CA de emissão a ser usado para o certificado de cliente e o modelo de certificado cliente RADIUS 'AMT 802.1X autenticação de cliente' e clique em OK.
   8. On 'Out of Band Management Properties "janela, clique em OK.
4. Diretiva de Grupo   
   ATENÇÃO: Devido a um erro no Windows 2008 R2 / Windows 7, este GPO deve ser criado em um Windows 2008 RTM MACHINE. CASO CONTRÁRIO, A GPO NÃO aplicar corretamente e você receberá um erro de conexão falha devido a "Validar certificado do servidor" ser erroneamente VERIFICADO.
   1. Criar uma nova política de grupo
      1. Configuração do computador | políticas | Configurações do Windows | Configurações de segurança | Serviços do sistema. Definir 'Wired AutoConfig' para Automático com segurança padrão.
      2. Configuração do computador | políticas | Configurações do Windows | Configurações de segurança | Rede com Fio (IEEE 802.3). Criar uma nova política de rede com fio.
         1. Nome da política
         2. Certifique-se de "serviço Use o Windows Wired Auto Config para os clientes" está marcada.
         3. Na guia Segurança:
            1. 'Ativar uso de autenticação IEEE 802.1X para acesso à rede' está marcada.
            2. método de autenticação de rede é "Microsoft: Protected EAP (PEAP)".
            3. Clique em "Propriedades":

Desmarque a opção "Validar certificado do servidor '

método de autenticação é "seguro senha (EAP-MSCHAP v2) '.

Clique em "Configurar ...". opção de logon do Windows garantir é verificada.

'Habilitar reconexão rápida "está marcada.

Fechar janela 'EAP Propriedades protegido'.

* + - * 1. Modo de autenticação é 'User re-autenticação ".
        2. 'Informações do usuário Cache para ligação subsequente a esta rede "está marcada.
        3. Clique "Avançadas ...":

"Activar Single Sign On para a rede" está marcada.

'Permitir diálogos adicionais a serem exibidos durante a Single Sign On' está desmarcada.

Fechar a janela 'configurações de segurança avançadas ".

* + - 1. Fechar janela de propriedades de política.

1. Dispositivos de Rede   
   NOTA: Esta configuração assume que RADIUS já está configurado para o interruptor para outros usos (ou seja, logins SSH). Se não, você vai precisar criar uma associação no servidor NPS e introduza o endereço do servidor e segredo compartilhado sobre a configuração do dispositivo. Chuck Murison tem um grande blog sobre como fazer isso em: <http://murison.wordpress.com/2010/11/11/cisco-radius-configuration-with-server-2008-r2/>
   1. Ativar RADIUS para 802.1X (no prompt de configuração global)
      1. raio aaa autenticação dot1x grupo padrão   
         Isso define o dispositivo para usar RADIUS para autenticação 802.1X
      2. aaa raio grupo padrão de rede autorização   
         Isso define o dispositivo para usar RADIUS para autorizar usuários para acesso específico
      3. autenticação mac-move autorização   
         Isso permite que as máquinas a ser movido enquanto uma sessão é aberta (dispositivo fecha sessão de idade)
      4. dot1x system-auth-control   
         Globalmente ativa a autenticação 802.1X
   2. Em uma base por porta, emitir os seguintes comandos (um comando de intervalo pode ser usado para configurar portas simultaneamente):
      1. mAb   
         Isto permite a autenticação MAC de bypass (onde necessário)
      2. a fim de autenticação dot1x mab   
         Isso informa ao dispositivo de rede para usar o 802.1X antes MAB
      3. autenticação prioridade dot1x mab   
         Isso informa ao dispositivo de rede para priorizar 802.1X antes MAB
      4. dot1x pae autenticador   
         Isso impede que o cliente linha descendente de tentar ser um suplicante
      5. A autenticação da porta do auto-controle   
         Esta liga 802.1X para a porta.
      6. Porto pode precisar de ser fechado / não fechada para forçar o cliente a autenticar.
   3. Siga-on ações
      1. Definir a VLAN padrão para a porta para outra coisa (ou seja, um convidado ou vlan offline). O VLAN é automaticamente comutada para a VLAN operações uma vez autenticado.
      2. Definir uma VLAN convidada para máquinas que estão sendo fotografados e ainda não capazes de autenticação 802.1X. Na interface:   
         dot1x guest-vlan <vlan-id>
      3. As configurações do dispositivo podem ter de ser ajustada para evitar tempo limite DHCP antes 802.1X timeout. As seguintes definições foram utilizadas com sucesso no laboratório de teste:
         1. dot1x tempo limite quiet-período de 3   
            Esta configuração é o tempo ocioso entre a autenticação falhou e a próxima tentativa.
         2. dot1x tempo limite tx-período de 5   
            Essa configuração é o tempo ocioso entre as transmissões.