Acceso a la red basado en la hora y autenticado con 802.1x

802.1x es un estándar del IEEE para controlar el acceso a una red por puerto. Los switches Cisco Small Business de la serie 300 admiten 802.1x para brindar una mayor seguridad de red. En una red compatible con 802.1x, cualquier dispositivo de usuario (como una computadora portátil o un teléfono IP) solicita acceso a los puertos al switch al que se encuentra directamente conectado. El switch obtiene la identificación y la contraseña del usuario (o del dispositivo) y los reenvía a un servidor RADIUS para su autenticación. El switch permite el acceso al puerto sólo si la autenticación del usuario es satisfactoria. El acceso autenticado a una LAN aumenta la seguridad de la red.

Productos destacados

Este consejo útil describe el uso de la autenticación basada en 802.1x en un switch administrado Cisco Small Business de la serie 300 (modelo SF300-48P), con varios puertos con y sin alimentación por Ethernet (PoE, Power over Ethernet). Para obtener más información sobre otros switches administrados Cisco de la serie 300, visite: http://www.cisco.com/go/300switches.

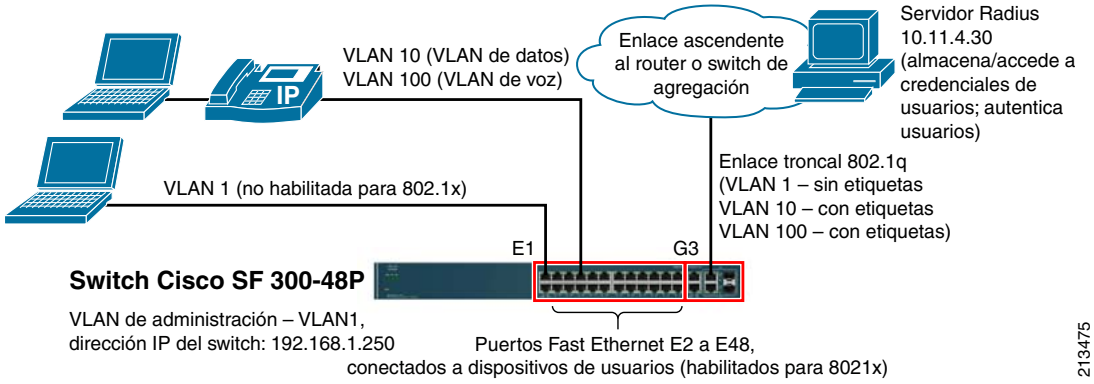
Diseño de red compatible con 802.1x

Los componentes principales de una red con autenticación basada en 802.1x, como se muestra en la Figura 1, son:

- Computadora portátil/teléfonos IP (u otros dispositivos similares para usuarios finales que puedan solicitar acceso a una red con base en 802.1x).
- Un switch que autentica al usuario mediante un servidor RADIUS y permite el acceso a la red solamente si la autenticación es exitosa.
- Un servidor RADIUS para autenticar al usuario.

Cuando se activa la autenticación 802.1x en una LAN, se suele hacerlo en todos los puertos del switch que se utilizan para conectar dispositivos de usuarios finales u otros dispositivos que requieren dicho acceso autenticado a puertos.

Figura 1 Acceso a la red autenticado con 802.1x



Autenticación

Para autenticar a un usuario, el servidor RADIUS accede a una base de datos de usuarios que contiene cierta información, como la identificación de usuario, la contraseña y otros datos opcionales que proporciona al switch al efectuarse la autenticación. La base de datos se puede integrar en el servidor RADIUS o funcionar de manera externa, como un Active Directory.

¿Qué puertos deben autenticarse?

La autenticación basada en 802.1x se usa principalmente para dispositivos para usuarios finales, como computadoras portátiles o teléfonos IP, que son dispositivos no confiables desde el punto de vista de la seguridad. Por eso, 802.1x no se configura en los puertos conectados a dispositivos de red, como routers, switches, servidores o cualquier otro dispositivo de confianza. Por el contrario, se configura en los puertos reservados para conectar dispositivos de usuarios a un switch de acceso y también a un switch de agregación, si se pueden conectar dispositivos de usuarios directamente a él.

Política de autenticación de puertos

El switch Cisco Small Business de la serie 300 puede configurarse con cualquiera de las siguientes tres políticas que definen cómo la autenticación basada en 802.1x afecta el acceso a los puertos cuando es posible conectar varios dispositivos en un mismo puerto:

- Host único: permite que solamente acceda al puerto un único host.
- Host múltiple (802.1x): el puerto admite varios hosts. Solamente se debe autorizar el primer host mediante 802.1x. Si la autorización es exitosa, tanto el dispositivo autorizado como todos los demás dispositivos conectados podrán acceder al puerto sin ninguna otra autenticación. Mientras no se autentique al menos un dispositivo conectado, ningún dispositivo puede acceder al puerto. Esto es útil para implementar dispositivos que no admiten 802.1x.
- Varias sesiones: permite que varios hosts accedan al puerto, pero cada uno debe autenticarse de manera individual y separada.

Nota La política de varias sesiones se recomienda en Cisco SMART Designs para obtener mayor flexibilidad y seguridad. La política de host múltiple puede usarse para admitir dispositivos en un puerto que no admite la autenticación 802.1 x.

Nota El switch Cisco Small Business de la serie 300 se puede configurar para colocar a un usuario en la VLAN para usuarios temporales cuando el usuario no aprueba la autenticación 802.1x.

Consideraciones del servidor RADIUS

El switch Cisco Small Business de la serie 300 accede al servidor RADIUS a través de la VLAN de administración, por medio de la dirección IP de administración individual asignada al switch (este último debe ser un switch de capa 3, compatible con varias interfaces IP). Esto implica que el switch debe poder utilizar su VLAN de administración para conectarse con el servidor RADIUS. Si el servidor RADIUS está en otra VLAN (como se supone en Figura 1), el router WAN realiza el routing entre VLAN necesario.

El router WAN marca el término de la VLAN de administración. Si se utiliza la VLAN de administración predeterminada de fábrica (VLAN 1), los switches LAN se deben configurar para reenviar la VLAN 1 sin etiquetas junto con otras VLAN, si corresponde, a través de sus puertos troncales hasta el router WAN.

Autenticación de teléfonos IP

Los teléfonos IP pueden autenticarse mediante 802.1x, al igual que las PC y las computadoras portátiles. Los teléfonos IP de Cisco son compatibles con 802.1x. Para obtener más información sobre la autenticación 802.1x del teléfono IP y la creación de ID de usuario apropiados para teléfonos IP en el servidor RADIUS, consulte la guía del administrador del teléfono IP específico.

Autenticación basada en la hora

El switch Cisco Small Business de la serie 300 permite restringir el acceso a los puertos compatibles con 802.1x a un determinado intervalo de tiempo, que especifica un intervalo de tiempo absoluto, por ejemplo, desde el 22 de febrero de 2010 a las 9 a. m. hasta el 30 de abril de 2023 a las 5 p. m. En este caso, se brinda a los usuarios acceso autenticado a los puertos en cualquier momento dentro del período especificado. Fuera de ese período, los puertos están en estado "Force Unauthorized" (Forzar restricción), que significa que no se puede acceder a ellos, y que no se ha realizado ninguna autenticación 802.1x.

Una vez que ha establecido un intervalo de tiempo absoluto, puede refinarlo agregándole un intervalo de tiempo recurrente. Este intervalo de tiempo recurrente restringe, además, el acceso de los usuarios a una determinada hora de inicio y finalización cada día de la semana (es posible definir períodos separados para los distintos días de la semana).

Se pueden agregar distintos intervalos de tiempo a los puertos. Esto es útil si las horas laborales (o las horas de acceso a la red) de los empleados varían.

Asignación de VLAN dinámica

La asignación de VLAN dinámica (DVA, Dynamic VLAN Assignment) otorga dinámicamente una VLAN específica de un usuario a un puerto luego de realizar la correspondiente autenticación 802.1x exitosa. La VLAN del usuario debe definirse en el perfil RADIUS del usuario. Al autenticarse al usuario con éxito, el servidor RADIUS proporciona al switch la información del usuario y la VLAN como parte del procedimiento de autenticación. Luego, el switch agrega el puerto como miembro sin etiqueta de esa VLAN. Esto permite la movilidad del usuario cuando diferentes usuarios pertenecen a VLAN de datos separadas en función de sus departamentos u otros criterios.

Si bien el switch Cisco Small Business de la serie 300 admite DVA, en este documento no se trata la configuración de esta función. Para obtener más información, consulte la guía del administrador en la siguiente dirección URL: http://www.cisco.com/en/US/docs/switches/lan/csbms/sf30x_sg30x/administration_guide/78-19308-01.pdf.

Consejos de configuración

En esta sección se ilustra un ejemplo de configuración de 802.1x para un switch Cisco Small Business de la serie 300. En particular, el ejemplo configura los puertos Fast Ethernet de e2 a e48 de un switch Cisco SF 300-48P para permitir el acceso autenticado a los puertos mediante 802.1x.

Esta sección hace referencia a la configuración de un switch de acceso en una topología Cisco SMART Design, como se muestra en la Figura 1.

Requisitos previos de la red para esta configuración

Requisitos previos de LAN

1. Todos los puertos de un switch Cisco Small Business de la serie 300 están asociados a la VLAN 1 nativa de forma predeterminada. En la práctica, suele ser necesario crear otras VLAN separadas para datos y voz. Este ejemplo de configuración usa la VLAN 10 como VLAN de datos y la VLAN 100 como VLAN de voz.

   A modo de ejemplo, se asigna un puerto (e1) a la VLAN 1 para utilizarlo como puerto de administración dedicado. Sin embargo, en la práctica, la VLAN 10 (VLAN de datos) también puede usarse como VLAN de administración. Además, el uso de puertos de administración dedicados es opcional.
2. Todas estas VLAN (VLAN 10, 100 y 1) terminan en el router WAN.
3. El switch Cisco de la serie 300 puede configurar un puerto de cualquiera de las siguientes tres maneras:
   - Puerto de acceso: El puerto se puede asociar a una sola VLAN, en cuyo caso se denomina ID de VLAN de puerto (PVID, Port VLAN ID). Un puerto de acceso reenvía todos los paquetes entrantes a través del puerto de la PVID. Solamente puede admitir una VLAN, por lo que no es apropiado si se usan VLAN de datos y voz por separado.
   - Puerto de enlace troncal: el puerto puede admitir una sola PVID y una o más VLAN encapsuladas (etiquetadas) con 802.1q. Como se ilustra en la Tabla 1, este diseño usa puertos de enlaces troncales.
   - Puerto general: este puerto puede admitir varias VLAN con y sin etiqueta, en cuyo caso el tráfico no etiquetado se reenvía a las VLAN según las direcciones MAC de origen.

Esta configuración supone que el switch de acceso está configurado tal como se ilustra en la Tabla 1. Los números de VLAN y puertos utilizados cambian en cada implementación según los requisitos específicos (consulte la Figura 1).

Tabla 1 Configuraciones de puerto para este ejemplo

	N.º de puerto	Tipo de puerto	VLAN de puerto (PVID)	VLAN etiquetadas	VLAN excluidas
Interfaz de administración de switch específica (opcional)	e1	Enlace troncal	VLAN 1		10, 100
Puertos conectados a computadoras portátiles/teléfonos IP de usuarios	e2 a e48	Enlace troncal	VLAN 10 (VLAN de datos)	VLAN 100 (VLAN de voz)	1
Puerto ascendente	G3 (también G1, G2, G4)	Enlace troncal	VLAN 1	VLAN 10, 100	1

4. El switch tiene activado el protocolo de árbol de expansión rápida y puede reenviar tráfico a través de la LAN mediante sus VLAN.

Configuración del switch de agregación

Esta configuración supone que el switch de agregación está configurado del modo descrito en la Tabla 2.

Tabla 2 Configuración del switch de agregación

	Puerto conectado al switch Cisco de la serie 300	Puerto conectado al router WAN
VLAN 1	Sin etiquetas (PVID)	Sin etiquetas (PVID)
VLAN 10	Con etiquetas	Con etiquetas
VALN 100	Con etiquetas	Con etiquetas

Nota Concretamente, verifique que el switch de agregación esté configurado para reenviar la VLAN 1 sin etiquetas (por ejemplo, si se usa un switch Cisco Catalyst, la VLANsin etiquetas debe incluirse en las VLAN que se permitirán a través del puerto de enlace troncal mediante un comando como switchport trunk allowed vlan 1,10,100).

Requisitos previos de configuración del router WAN

Se presupone que el router WAN marca el término de las VLAN, tal como se ilustra en la Tabla 3.

Tabla 3 Terminación de VLAN en el router WAN

	Puerto del router conectado al switch Cisco de la serie 300	
	Tipo de interfaz VLAN	Dirección IP (puerta de enlace predeterminada para la subred)
VLAN 1	VLAN nativa (sin etiquetas)	192.168.1.1
VLAN 10	Con etiquetas	10.1.20.1
VLAN 100	Con etiquetas	10.1.100.1

Requisitos previos de la configuración del servidor RADIUS

1. Verifique que el servidor RADIUS esté configurado para aceptar solicitudes de autenticación RADIUS para el switch específico; es decir, que la dirección IP del switch y la cadena de clave (contraseña compartida) se especifiquen en el servidor RADIUS. Esto implica configurar lo siguiente en el servidor RADIUS:
   - Los puertos UDP utilizados por el servidor RADIUS para escuchar las solicitudes de autenticación RADIUS y las autorizaciones RADIUS (por lo general, son los puertos 1812/1813 o 1645/1646). Deben coincidir entre el servidor RADIUS y todos los switches compatibles con 802.1x.
   - La dirección IP del servidor de acceso a la red (NAS, Network Access Server). El NAS es el cliente que envía solicitudes de autenticación RADIUS al servidor RADIUS. En este caso, el switch envía las solicitudes de autenticación de usuarios al servidor RADIUS, por lo cual es el NAS. En consecuencia, el servidor RADIUS se debe configurar con la dirección IP de cada switch que ejecute operaciones de autenticación basadas en 802.1x en la red.
   - Cadena de clave: se trata de una cadena alfanumérica utilizada por el servidor RADIUS para autenticar el NAS específico. La misma cadena de clave se debe configurar también en el switch correspondiente como parte de la configuración del switch (ver a continuación).
2. Verifique que el switch pueda conectarse (hacer ping) con el servidor RADIUS. El switch habla con el servidor RADIUS a través de la VLAN de administración (VLAN 1, en este ejemplo) y utiliza su dirección IP de administración como la dirección IP de origen.
3. Verifique que el servidor RADIUS tenga configurado, al menos, un perfil de usuario (ID de usuario y contraseña) para fines de prueba (luego se pueden agregar otros usuarios). Por lo general, la información mínima sobre el usuario configurada en un servidor RADIUS como Cisco ACS comprende:
   - ID de usuario
   - Grupo de usuarios: grupos creados por administradores, tales como empleados habituales, administradores de red, gerentes, encargadados del departamento de cuentas, entre otros.
   - Contraseña de usuario
   - El tipo de autenticación (PAP/CHAP, etc.) asociado al grupo de usuarios.
   - La lista de atributos RADIUS (diccionario RADIUS) admitida para el grupo de usuarios, si el servidor RADIUS admite más de una lista.

Nota Los campos exactos necesarios para el perfil de usuario pueden variar según el servidor RADIUS. De manera opcional, se puede configurar un grupo de usuarios en un servidor RADIUS con información adicional, mientras se establece la conexión del usuario. Por ejemplo, el grupo de usuarios puede especificar una VLAN que se utilizará como PVID del puerto del switch una vez autenticado el usuario.

Configuración del switch para usar un servidor RADIUS

Esta configuración habilita la autenticación RADIUS en el switch y configura 802.1x en los puertos del switch e2 a e48.

Mientras configura el switch, guarde cada tanto la configuración en el archivo de configuración de inicio, ya que las configuraciones no guardadas se pierden si se reinicia el switch. Para guardar la configuración, siga los pasos descritos a continuación:

Paso 1 Seleccione **Administration (Administración) > File Management (Administración de archivos) > Copy/Save Configuration (Copiar/guardar configuración)**.

Se abrira la página de copiar/guardar configuración.

Paso 2 Seleccione el nombre del archivo de origen que se copiará como *Running configuration* (Configuración en ejecución).

Paso 3 Seleccione el nombre de archivo de destino como *Startup configuration* (Configuración de inicio).

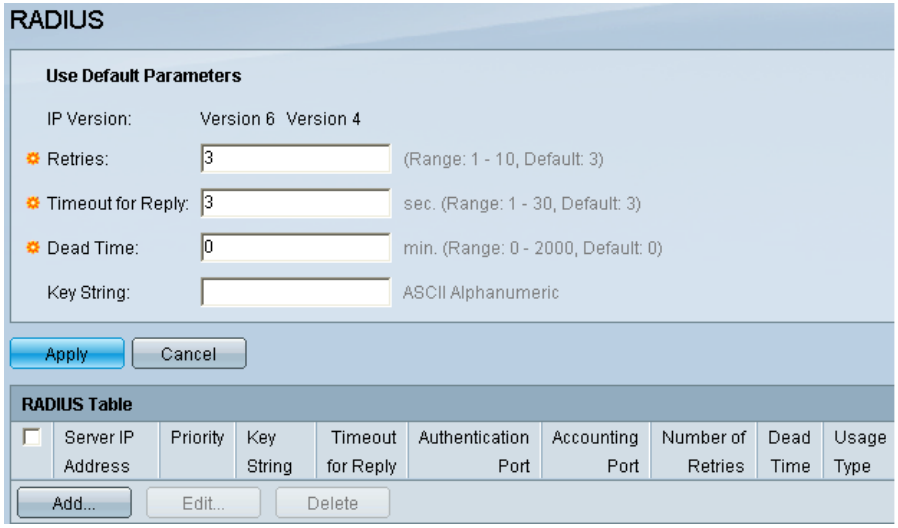
Paso 4 Haga clic en **Apply** (Aplicar). Se guardará el archivo de configuración.

Para configurar el switch a fin de utilizar un servidor RADIUS, siga los pasos descritos a continuación.

Paso 1 **Paso 1** Seleccione **Security (Seguridad) > RADIUS**.

Se abre la pantalla RADIUS (Figura 2).

Figura 2 Pantalla RADIUS

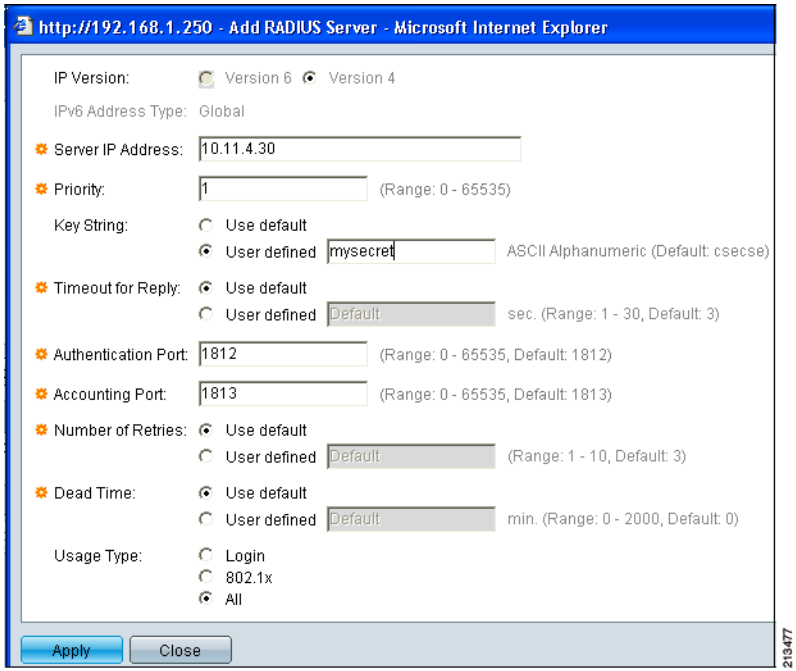


Este paso especifica los detalles del servidor RADIUS (dirección IP y cadena de clave) al switch, de modo tal que el switch pueda comunicarse con él. Verifique que aún no se hayan configurado los detalles del servidor RADIUS en el switch; es decir, que no aparezcan detalles del servidor RADIUS debajo de la tabla RADIUS (de lo contrario, puede utilizar el servidor RADIUS actual).

Paso 2 Para agregar información de un nuevo servidor RADIUS en el switch, haga clic en **Add** (Agregar).

Se abre la ventana emergente en la Figura 3.

Figura 3 Cómo agregar información de un nuevo servidor RADIUS



Paso 3 Ingrese la siguiente información:

a. Dirección IP del servidor: la dirección IP del servidor RADIUS.

b. Prioridad: 1 (el primer servidor RADIUS que debe contactarse).

c. Cadena de clave: la contraseña compartida configurada en el servidor RADIUS para este switch. El servidor RADIUS autentica el switch que utiliza esta contraseña antes de realiza cualquier autenticación de usuario.

d. Autenticación y puertos de acceso: estos valores predeterminados deben modificarse si el servidor RADIUS se configura para comunicarse a través de otros puertos UDP.

e. Tipo de uso: seleccione **All** (Todos) para que RADIUS se use para realizar autenticaciones basadas en 802.1x y de inicio de sesión.

Paso 4 Haga clic en **Close** (Cerrar) para quitar la ventana emergente.

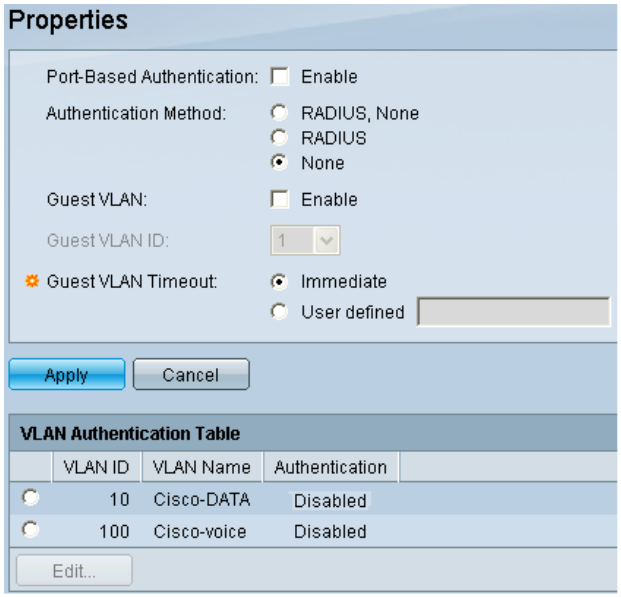
La tabla RADIUS de la pantalla RADIUS ahora muestra información del nuevo servidor RADIUS.

Configuración del switch para acceso autenticado a puertos basado en 802.1x

Paso 1 Seleccione **Security (Seguridad) > 802.1x > Properties (Propiedades)**.

Se abrirá la pantalla de propiedades (Figura 4).

Figura 4 Pantalla de propiedades



Los siguientes pasos permiten activar 802.1x en las VLAN seleccionadas y especificar RADIUS como política de autenticación para 802.1x.

Paso 2 En la pantalla de propiedades, haga lo siguiente:

a. Port-based Authentication (Autenticación basada en puertos): Haga clic en **Enable** (Habilitar)

b. Authentication Method (Método de autenticación)**:** seleccione **RADIUS** para indicar la autenticación RADIUS obligatoria. Si el servidor RADIUS rechaza la autenticación o no está disponible, la sesión no se permite.

La opción "RADIUS, None" (RADIUS, ninguna) es similar porque el rechazo de la autenticación finaliza la sesión. Sin embargo, si la autenticación RADIUS no pude realizarse (servidor/red no disponible), la sesión se permite.

c. Guest VLAN (VLAN para usuarios temporales)**:** no se usa en este ejemplo.

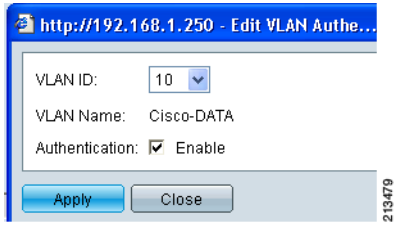
Paso 3 Haga clic en **Apply** (Aplicar) y verifique que la operación se haya realizado con éxito.

La tabla de Autenticación de VLAN al final de la pantalla de propiedades muestra las VLAN y si está habilitada la autenticación 802.1x en cada una de ellas (de forma predeterminada, puede estar habilitada).

Paso 4 En la pantalla de propiedades, seleccione **VLAN 10** y haga clic en **Edit** (Editar).

Se abre la pantalla emergente que se ilustra en la Figura 5.

Figura 5 Pantalla de edición de VLAN



Paso 5 Haga lo siguiente:

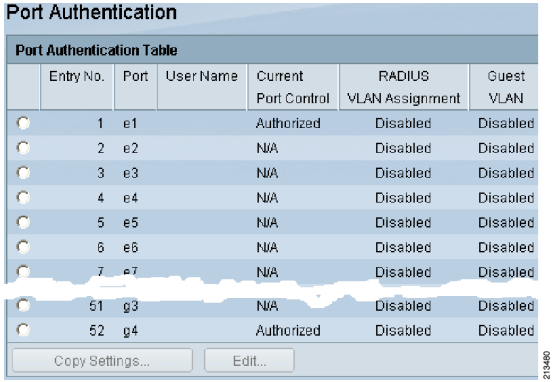
- Si el campo "Authentication" (Autenticación) muestra que 802.1x está deshabilitada en VLAN 10, haga clic en **Enable** (Habilitar) para habilitar 802.1x en VLAN 10. Luego, haga clic en **Apply** (Aplicar) y verifique que la operación se haya realizado con éxito.
- Si desea habilitar la autenticación 802.1x para teléfonos IP, active 802.1x en VLAN 100 del mismo modo. Para ello, seleccione **VLAN 100** en esta pantalla, haga clic en **Enable** (Activar) y luego en **Apply** (Aplicar).

Verifique en la pantalla de propiedades que se haya habilitado la autenticación 802.1x en las VLAN correspondientes.

Paso 6 Seleccione **Security (Seguridad) > 802.1x > Port Authentication (Autenticación de puertos)**.

Se abre la pantalla de autenticación de puertos que se ilustra en la Figura 6.

Figura 6 Pantalla de autenticación de puertos



Aunque se haya habilitado 802.1x en las VLAN, esta pantalla permite realizar más configuraciones por puerto. Cada puerto puede configurarse de cualquiera de las siguientes maneras:

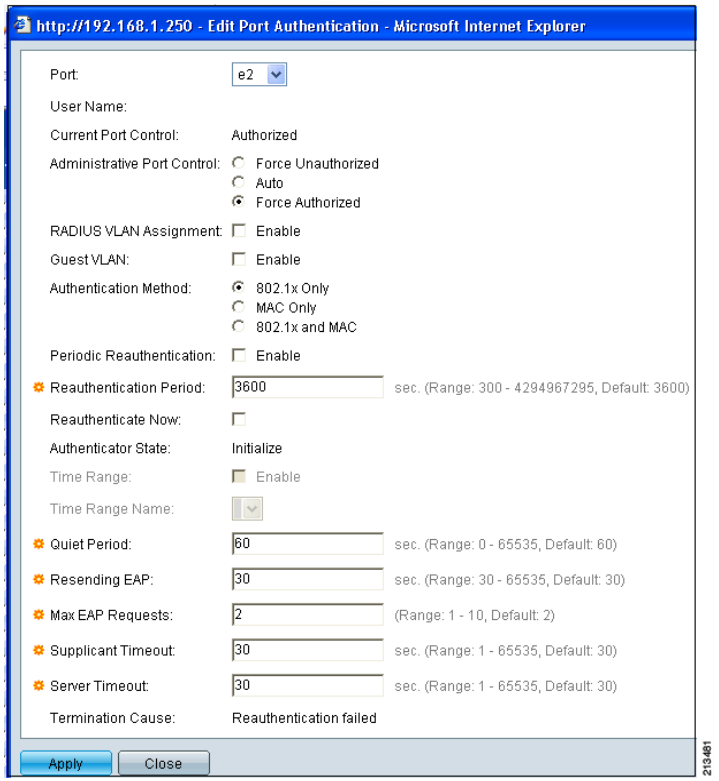
- Force Authorized (Autorización forzada): el acceso al puerto se permite siempre (desactivar 802.1x en este puerto)
- Force Unauthorized (Restricción forzada): no se permite acceder a través del puerto.
- Auto (Automático): se permite el acceso a través del puerto solamente si la autenticación 802.1x es exitosa.

Si bien el puerto debe estar en modo automático para que se realice la autenticación 802.1x, antes de activar el modo para el intervalo de puertos, es necesario configurar otros parámetros en estos puertos que requieren que los puertos estén en modo de restricción forzada. Por eso, antes de proceder, es importante asegurarse de que el intervalo de puertos se encuentre en modo de autorización forzada.

Paso 7 Seleccione el puerto **e2** y haga clic en **Edit** (Editar).

Se abre la pantalla de edición de la autenticación de puertos que se ilustra en la Figura 7.

Figura 7 Pantalla de edición de la autenticación de puertos



Paso 8 Ingrese los siguientes valores en los campos, según se muestra en la Figura 7:

- Administrative Port Control (Control administrativo de puertos): seleccione **Force Authorized**.
- Authentication Method (Método de autenticación): seleccione **802.1x Only (Solamente 802.1x)**.
- De ser necesario, puede activar también la reautenticación periódica. No modifique los valores predeterminados, tal como se muestra en la Figura 7.

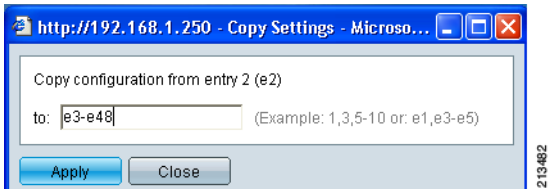
Paso 9 Haga clic en **Apply** (Aplicar). Verifique que aparezca la palabra "Success" (Resultado satisfactorio) en la pantalla.

Paso 10 Haga clic en **Close** (Cerrar) para cerrar la pantalla emergente y mostrar la pantalla subyacente de autenticación de puertos.

Paso 11 En la pantalla de autenticación de puertos, seleccione el puerto **e2** y haga clic en **Copy Settings** (Copiar configuración).

Se abrirá la ventana emergente de copiar configuración que se ilustra en la Figura 8.

Figura 8 Ventana emergente de copiar configuración



Paso 12 Ingrese el intervalo de puertos (por ejemplo, **e3–e48**) para copiar la configuración de e2.

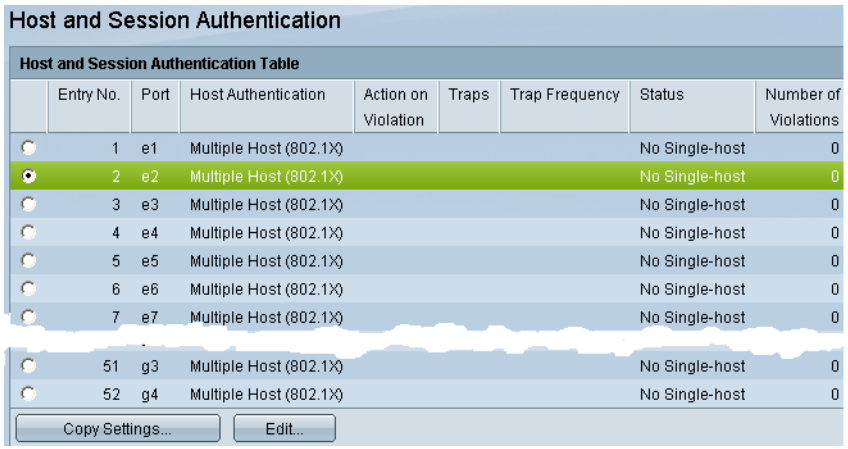
Paso 13 Haga clic en **Apply** (Aplicar) y verifique que aparezca la palabra "Success" (Resultado satisfactorio) en la pantalla de autenticación de puertos.

Esto permite colocar los puertos del intervalo de puertos en el modo de autorización forzada.

Paso 14 Seleccione **Security (Seguridad) > 802.1x > Hosts and Session Authentication (Autenticación de hosts y sesiones)**.

Se abre la pantalla de autenticación de hosts y sesiones Figura 9), que permite especificar las políticas de acceso que se aplicarán cuando se conecta más de un dispositivo al puerto.

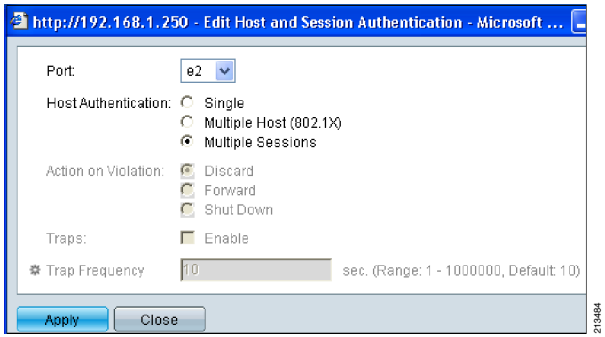
Figura 9 Pantalla de autenticación de hosts y sesiones



Paso 15 Para cambiar la política del puerto **e2**, seleccione el puerto **e2**, como se muestra en la Figura 9, y haga clic en **Edit** (Editar).

Se abrirá la pantalla de edición de autenticación de hosts y sesiones que se ilustra en la Figura 10.

Figura 10 Pantalla emergente de edición de autenticación de hosts y sesiones



Paso 16 En el campo Host Authentication (Autenticación de hosts), seleccione **Multiple Sessions** (Varias sesiones) y haga clic en **Apply** (Aplicar).

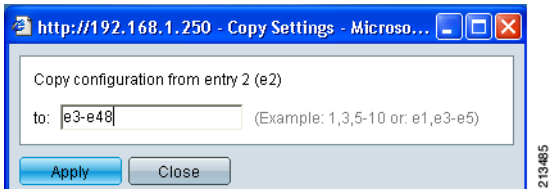
Verifique que aparezca la palabra "Success" (Resultado satisfactorio).

Si la operación se rechaza, vuelva al Paso 7, cambie el valor del campo Administrative Port Control (Control administrativo de puertos) a **Force Authorized** (Autorización forzada) e inténtelo nuevamente.

Paso 17 En la pantalla de autenticación de hosts, seleccione el puerto **e2** y haga clic en **Copy Settings** (Copiar configuración).

Se abrirá la ventana emergente de copiar configuración que se ilustra en la Figura 11.

Figura 11 Pantalla emergente de copiar configuración



Paso 18 Ingrese el intervalo de puertos (por ejemplo, **e3–e48**) para copiar la configuración de e2 a los puertos especificados, y haga clic en **Apply** (Aplicar).

Verifique que aparezca la palabra "Success" (Resultado satisfactorio) en la pantalla de autenticación de hosts y sesiones.

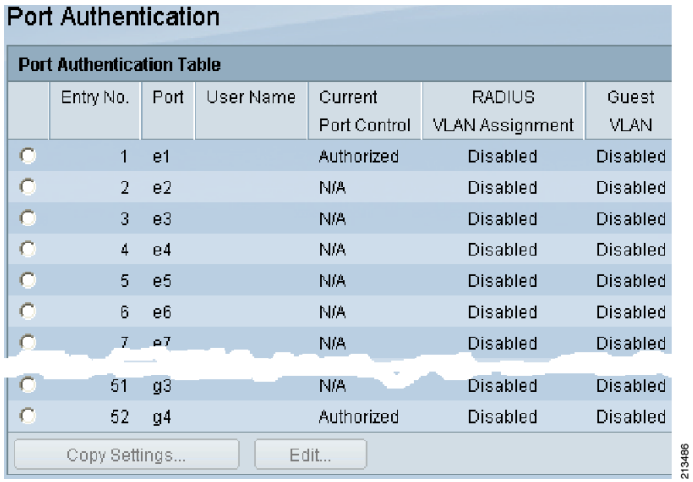
Esto permite colocar los puertos del intervalo de puertos en el modo de varias sesiones de la autenticación de hosts.

El paso siguiente activa la autenticación 802.1x en un solo puerto (e2) para poder realizar la verificación. Después de verificar que funciona, 802.1.x se habilitaría en otros puertos.

Paso 19 Para activar la autenticación 802.1x en el puerto e2, seleccione **Security (Seguridad) > 802.1x > Port Authentication (Autenticación de puertos)**.

Se abrirá la pantalla de autenticación de puertos, como se ilustra en la Figura 12.

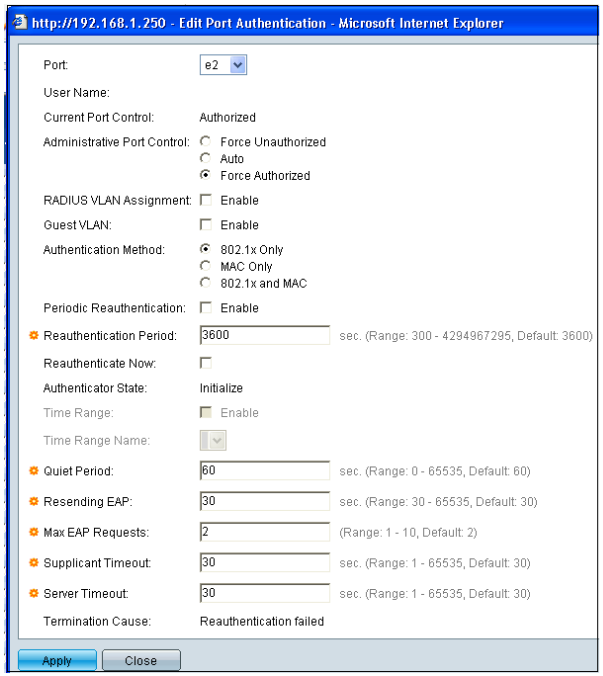
Figura 12 Pantalla de autenticación de puertos



Paso 20 Seleccione el puerto **e2** y haga clic en **Edit** (Editar).

Se abre la pantalla de edición de la autenticación de puertos que se ilustra en la Figura 13.

Figura 13 Pantalla de edición de la autenticación de puertos



Paso 21 Ingrese los siguientes valores en los campos:

- Administrative Port Control (Control administrativo de puertos): seleccione **Auto (Automático)**.
- Authentication Method (Método de autenticación): seleccione **802.1x Only (Sólo 802.1x)**.
- De ser necesario, puede activar también la reautenticación periódica. Mantenga los valores predeterminados de los tiempos de espera agotados, como se muestra en la Figura 13.

Paso 22 Haga clic en **Apply** (Aplicar) y verifique que aparezca la palabra "Success" (Resultado satisfactorio) en la pantalla.

Paso 23 Haga clic en **Close** (Cerrar) para cerrar la pantalla emergente y mostrar la pantalla subyacente de autenticación de puertos.

Con esto, finaliza la configuración de 802.1x en el puerto e2.

Paso 24 Para verificar el funcionamiento de 802.1x en el puerto e2, conecte una computadora portátil al puerto e2 y configure la conexión Ethernet de la computadora de la siguiente manera:

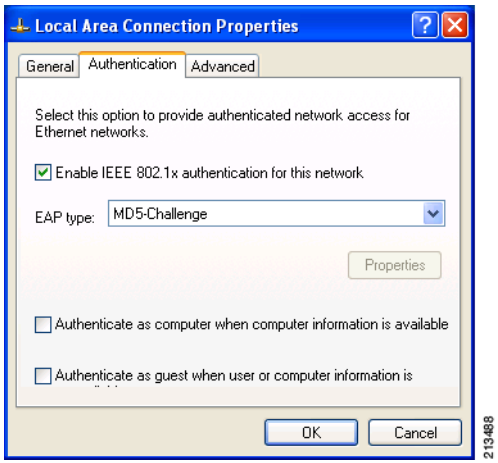
- Acepte una dirección IP y un DNS mediante DHCP.
- Realice una autenticación 802.1x.

Las pantallas puede variar según el tipo y la versión de sistema operativo de la computadora portátil. El ejemplo ilustrado en este documento es para Windows XP.

Paso 25 Seleccione **Local Area Connection Properties (Propiedades de conexión de área local) > General > Authentication (Autenticación)**.

Se abre la ventana mostrada en la Figura 14.

Figura 14 Propiedades de conexión de área local: ficha Authentication (Autenticación)



Paso 26 Seleccione la **autenticación IEEE 802.1x**.

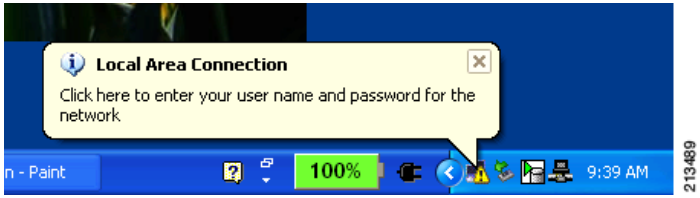
Paso 27 Seleccione el tipo de EAP como **MD5-Challenge** o **PEAP**, según corresponda.

Este debe coincidir con el tipo de autenticación del grupo de usuarios configurada en el servidor RADIUS.

Paso 28 Haga clic en **OK** (Aceptar) para guardar los cambios de configuración

Durante unos segundos después de conectarla, la computadora portátil puede mostrar que la conexión se encuentra activa, aunque no permita el acceso del usuario. Al cabo de unos segundos, debería aparecer un mensaje que solicita ingresar el nombre de usuario y la contraseña, como se ilustra en la Figura 15.

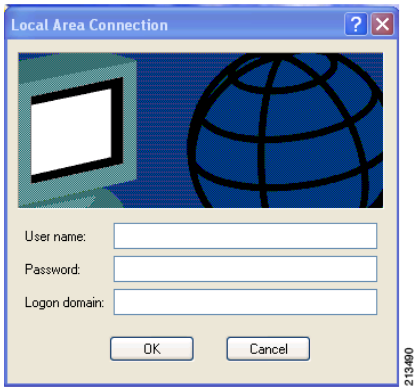
Figura 15 Ingreso de nombre de usuario y contraseña



Paso 29 Haga clic en el icono indicado.

Se abrirá la pantalla ilustrada en la Figura 16 para ingresar el nombre de usuario y la contraseña para la autenticación.

Figura 16 Pantalla de autenticación de usuario



Paso 30 Ingrese el nombre de usuario y la contraseña, y haga clic en **OK** (Aceptar).

La autenticación basada en 802.1x se realiza satisfactoriamente y el icono de conexión de la computadora portátil situado en la barra de tareas indica una conexión exitosa.

Paso 31 Seleccione **Security (Seguridad) > 802.1x > Port Authentication (Autenticación de puertos)**.

Se abrirá la pantalla de autenticación de puertos (Figura 12) con una tabla que especifica el estado autenticado de los puertos. Verifique que el puerto e2 figure en la lista en estado "Authorized"(Autorizado) en la columna "Current Port Control" (Control actual de puertos).

Paso 32 Seleccione **Security (Seguridad) > 802.1x > Authenticated Hosts (Hosts autenticados)**.

Se abrirá la pantalla de hosts autenticados, que muestra cada puerto actualmente autenticado mediante 802.1x. Por cada puerto autenticado, se muestra la identificación de usuario correspondiente, la dirección MAC del dispositivo de usuario (como una computadora portátil) y el tiempo de la sesión. Verifique que la información mostrada aquí con respecto al puerto e2 sea correcta.

Ahora puede hacer ping a las direcciones IP de la red para verificar si el puerto permite el tráfico del usuario.

Con esto, finaliza la verificación de 802.1x en el puerto e2.

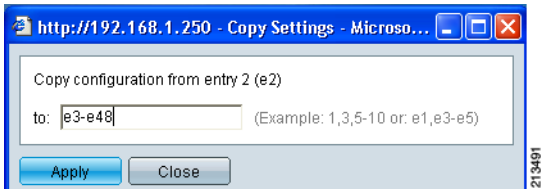
Paso 33 Para activar la autenticación 802.1x en otros puertos (puertos e2–e48, en este ejemplo), seleccione **Security (Seguridad) > 802.1x >Port Authentication (Autenticación de puertos)**.

Se abrirá la pantalla de autenticación de puertos.

Paso 34 Seleccione el puerto **e2** y haga clic en **Copy Settings (Copiar configuración)**.

Se abrirá la ventana emergente de copiar configuración que se ilustra en la Figura 17.

Figura 17 Pantalla emergente de copiar configuración



Paso 35 Ingrese el intervalo de puertos (por ejemplo, **e3–e48**) para copiar la configuración de e2 a los puertos especificados, y haga clic en **Apply** (Aplicar).

Verifique que aparezca la palabra "Success" (Resultado satisfactorio) en la pantalla de autenticación de puertos.

Esto activa 802.1x en el intervalo de puertos especificado.

Configuración de acceso a puertos en función de un intervalo de tiempo (opcional)

Estos ajustes permiten configurar un puerto para un intervalo de tiempo absoluto del 17 de agosto de 2010 al 1 de enero de 2020. También restringe el acceso del usuario a determinados períodos durante cada día de la semana (por ejemplo, de 9 a. m. a 5 p. m. el lunes).

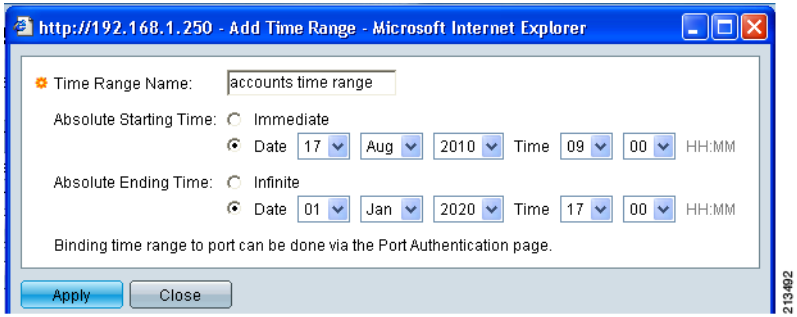
Paso 1 Seleccione **Security (Seguridad) > 802.1x > Time Range (Intervalo de tiempo)**.

Se abrirá la pantalla de intervalo de tiempo para agregar un intervalo de tiempo absoluto.

Paso 2 Haga clic en **Add** (Agregar).

Se abre la pantalla emergente mostrada en la Figura 18.

Figura 18 Cómo agregar un intervalo de tiempo



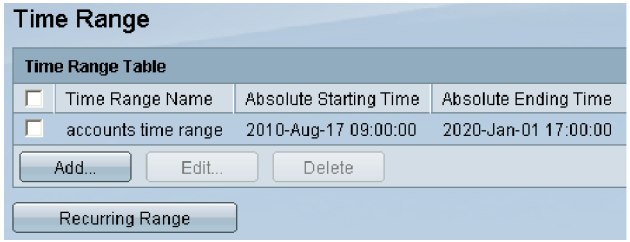
Paso 3 Ingrese un nombre para el intervalo de tiempo absoluto (**intervalo de tiempo de cuentas**), y la hora de inicio, hora de finalización, fecha de inicio y fecha de finalización del período, como se muestra en la Figura 18.

Si lo desea, puede especificar la hora de inicio como inmediata o la hora de finalización como infinita.

Paso 4 Haga clic en **Apply** (Aplicar) y verifique que aparezca la palabra "Success" (Resultado satisfactorio).

Se abrirá la pantalla mostrada en la Figura 19, que contiene una lista del intervalo de tiempo ingresado recientemente.

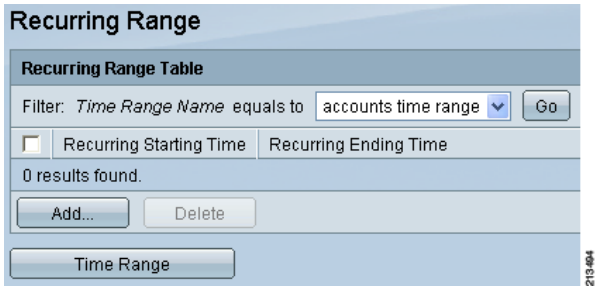
Figura 19 Pantalla de intervalo de tiempo



Paso 5 Haga clic en **Recurring Range** (Intervalo recurrente).

Se abrirá la pantalla de intervalo de tiempo recurrente, ilustrada en la Figura 20.

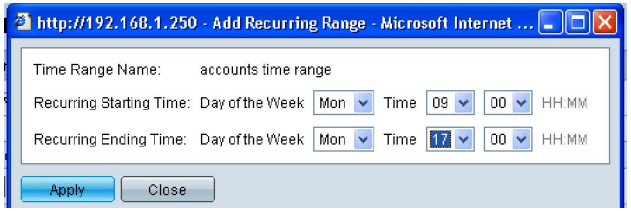
Figura 20 Pantalla de intervalo recurrente



Paso 6 Haga clic en **Agregar**.

Se abrirá la pantalla para agregar intervalo recurrente, como se muestra en la Figura 21, que permite agregar uno o más intervalos de tiempo recurrentes al intervalo de tiempo absoluto seleccionado (intervalo de tiempo de cuentas, en este ejemplo).

Figura 21 Figura 23



Paso 7 Ingrese los valores "Recurring Starting Time" (Hora de inicio recurrente) y "Recurring Ending Time" (Hora de finalización recurrente) para cualquier día de la semana, como se muestra en la Figura 21 y haga clic en **Apply** (Aplicar).

Verifique que aparezca la palabra "Success" (Resultado satisfactorio).

Tal como se ilustra en la Figura 21, esto crea un intervalo de tiempo recurrente para el lunes de 9 a. m. a 5 p. m., lo cual permite acceder a la red únicamente durante este período en tanto la autenticación 802.1x sea exitosa.

Repita los pasos 5 y 6 para agregar más intervalos de tiempo recurrentes para los demás días de la semana.

Con esto, concluye la creación del intervalo de tiempo. Ahora debe aplicarlo a los puertos.

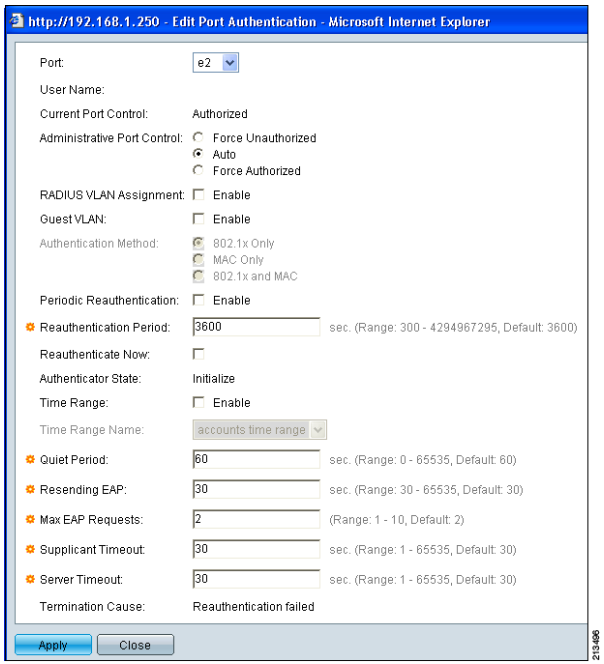
Paso 8 Seleccione **Security (Seguridad) > 802.1x > Port Authentication (Autenticación de puertos)**.

Se abrirá la pantalla de autenticación de puertos con una lista de todos los puertos y detalles de ellos.

Paso 9 Seleccione un puerto (**e2**, en este ejemplo) al que aplicará el intervalo de tiempo y haga clic en **Edit** (Editar).

Se abre la pantalla ilustrada en la Figura 22 con los detalles del puerto. Hay que tener en cuenta que el campo "Time Range" (Intervalo de tiempo) no está habilitado en esta pantalla de forma predeterminada.

Figura 22 Pantalla de edición de la autenticación de puertos



Paso 10 Para agregar el intervalo de tiempo al puerto e2, haga lo siguiente:

a. Haga clic para habilitar el campo "Time Range" (Intervalo de tiempo).

b. En el campo "Time Name Range" (Nombre del intervalo de tiempo), seleccione un intervalo de tiempo de la lista desplegable (en este caso, intervalo de tiempo de cuentas).

Paso 11 Haga clic en **Apply** (Aplicar).

Verifique que aparezca la palabra "Success" (Resultado satisfactorio) en la pantalla de edición de la autenticación de puertos.

Paso 12 Haga clic en **Close** (Cerrar) para cerrar la pantalla de edición de la autenticación de puertos.

El puerto e2 ahora está configurado con el intervalo de tiempo.

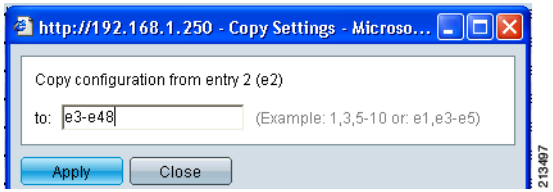
Paso 13 Seleccione **Security (Seguridad) > 802.1x > Port Authentication (Autenticación de puertos)**.

Se abrirá la pantalla de autenticación de puertos con una lista de todos los puertos y detalles de ellos. Esto permite copiar la configuración del puerto e2 a otros puertos similares.

Paso 14 Seleccione un puerto (e2, en este ejemplo) al que se haya aplicado el intervalo de tiempo y haga clic en **Copy Settings** (Copiar configuración).

Se abrirá la pantalla ilustrada en la Figura 23, que permite ingresar el intervalo de puertos en que se copiará la configuración del puerto e2.

Figura 23 Pantalla de copiar configuración



Paso 15 Ingrese el intervalo (por ejemplo, e2–e48) y haga clic en **Apply** (Aplicar).

Esta pantalla desaparece y la pantalla de autenticación de puertos se actualiza.

Paso 16 Verifique que aparezca la palabra "Success" (Resultado satisfactorio) en la pantalla de autenticación de puertos.

Con esto, concluye la configuración de 802.1x para los puertos e2 a e48.

Resumen

Este documento describe el uso de la autenticación 802.1x y su configuración en un switch Cisco Small Business de la serie 300. Esto permite el acceso autenticado a los puertos de la LAN, lo cual aumenta el nivel de seguridad de la red. Para mejorar la seguridad aún más, admite el acceso basado en la hora que restringe el acceso a los puertos determinados durante ciertas horas del día. Además, la asignación de VLAN dinámica puede aprovecharse para asignar automáticamente la VLAN a un usuario, de modo que no sea necesario configurar con anterioridad los puertos con las VLAN. Estos pasos facilitan la implementación de LAN con mayores niveles de seguridad y flexibilidad.

Si desea obtener más información sobre la configuración de switches administrados Cisco de la serie 300, consulte la Guía del administrador en la siguiente dirección URL:

http://www.cisco.com/en/US/docs/switches/lan/csbms/sf30x_sg30x/administration_guide/78-19308-01.pdf