Configurar el 802.1x en el Switches de las SG300 Series

Objetivo

el 802.1x es un estándar de IEEE que los instrumentos puerto-basaron la autenticación. Si un 802.1x de los USO de puertos, entonces cualquier cliente que utilice ese puerto (designado el suplicante) debe presentar las credenciales correctas antes de ser concedida el acceso a la red. Un dispositivo que ejecuta el 802.1x (designado el authenticator) debe poder comunicar con un servidor RADIUS (servicio del usuario de acceso telefónico con autenticación remota) que esté a otra parte en la red. Este servidor contiene una lista de usuarios válidos que no se prohiban el acceso a la red; cualquier credencial enviada por el authenticator (dado a él por el suplicante) debe hacer juego los que está sostenidos por el servidor de RADIUS. Si es así el servidor dice el authenticator conceder el acceso al usuario; si no, el authenticator negará el acceso.

El estándar del 802.1x es una buena medida de Seguridad en evitar que los usuarios indeseados accedan a la red enchufando a un puerto físico. Observe por favor eso para que el 802.1x trabaje, un servidor de RADIUS debe ser configurado ya a otra parte en la red, y el authenticator debe poder comunicar con él.

El objetivo de este documento es mostrarle cómo poner el 802.1x en el Switches de las SG300 Series.

Dispositivos aplicables

- Switches de las SG300 Series

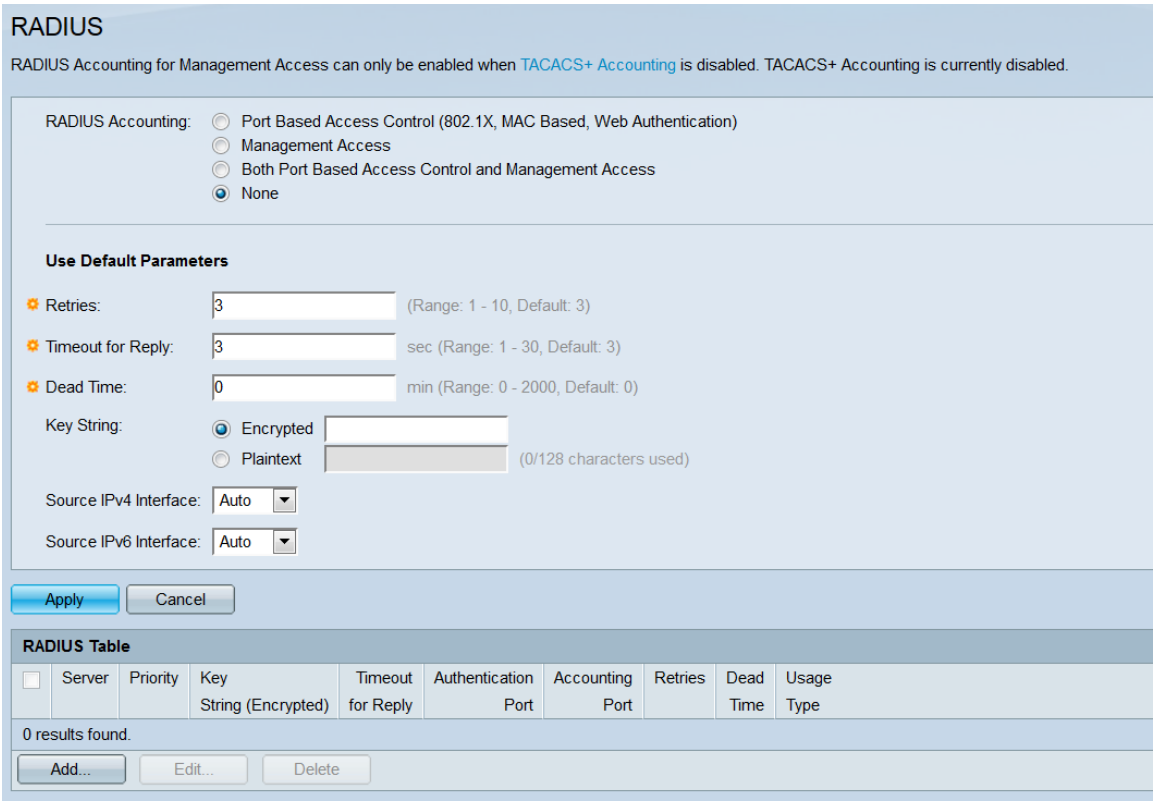
Versión de software

- v1.4.1.3

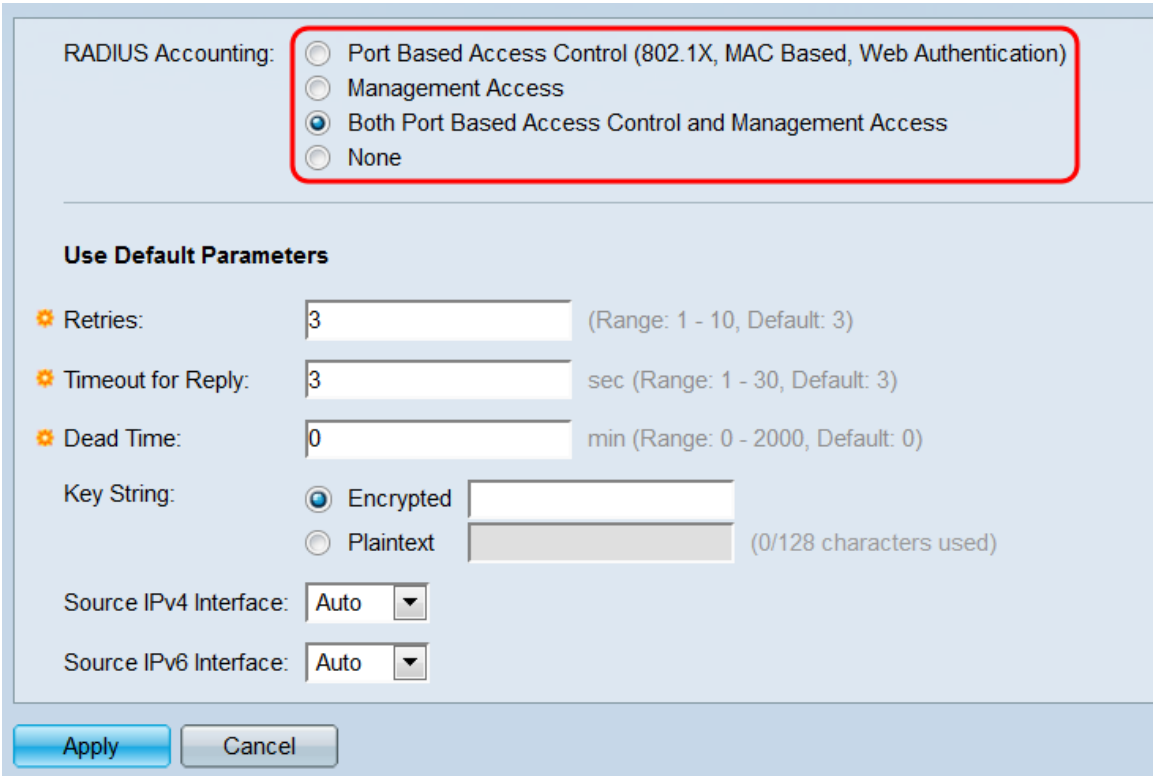
Determinación de la autenticación del 802.1x

Agregar a un servidor de RADIUS

Paso 1. Ábrase una sesión a la utilidad de configuración de la red y elija la **Seguridad > el RADIUS**. La página *RADIUS* se abre.



Paso 2. En el campo de las *estadísticas RADIUS*, elija un botón de radio para seleccionar qué tipo de información de la cuenta darán el servidor de RADIUS. Un servidor de RADIUS puede ser dado la información de la cuenta que no pierde de vista el tiempo de la sesión de un usuario, qué recursos utilizan, y otras cosas. La opción seleccionada aquí no afectará el funcionamiento del 802.1x.



Las opciones son:

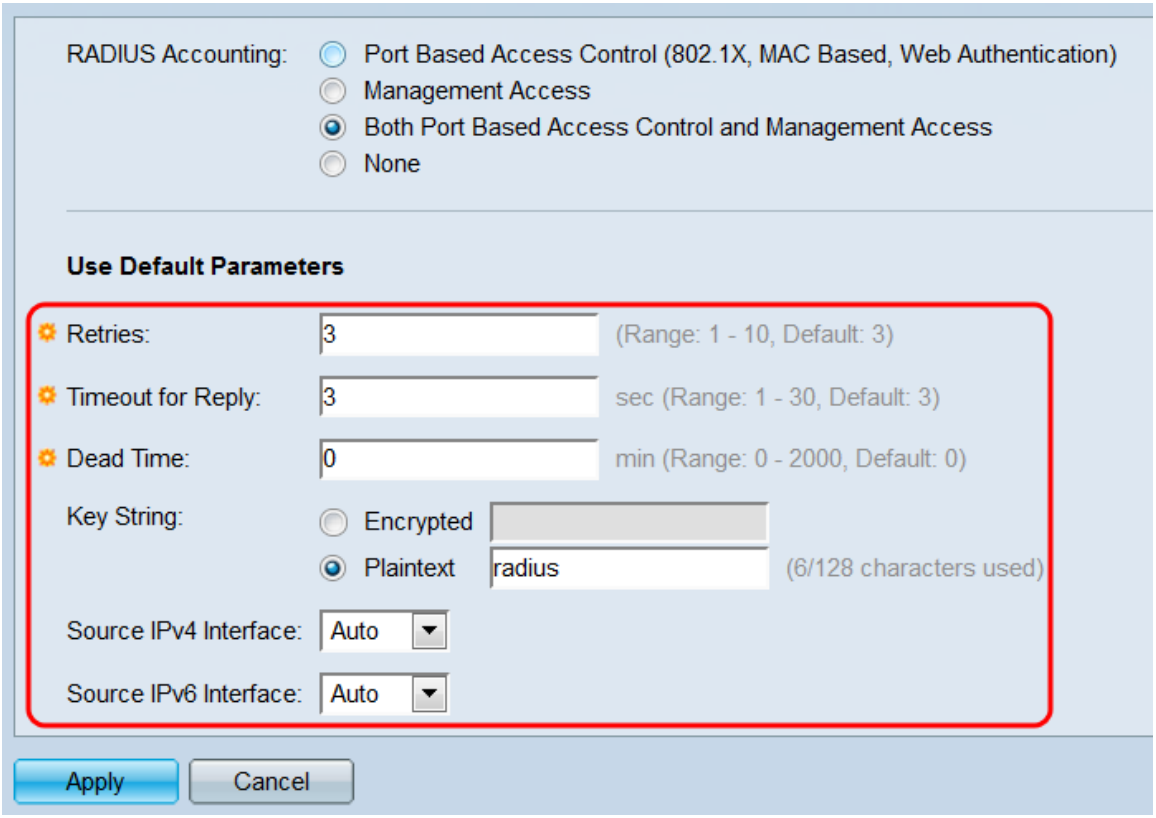
- El puerto basó el control de acceso – Esta opción envía la información de la cuenta sobre las sesiones autenticadas puerto-basadas al servidor de RADIUS.

• Acceso de administración – Esta opción envía la información de la cuenta sobre las Sesiones de administración del conmutador al servidor de RADIUS.

• El puerto basó el control de acceso y el Acceso de administración – Esta opción envía ambos tipos de información de la cuenta al servidor de RADIUS.

• Ninguno – No envíe la información de la cuenta al servidor de RADIUS.

Paso 3. En la *área de parámetros del valor por defecto del uso*, configure las configuraciones que serán utilizadas por abandono a menos que configuren a un servidor de RADIUS agregado con sus propias configuraciones específicas; cada entrada del servidor individual que usted agrega al conmutador puede utilizar los valores por defecto o separar las configuraciones únicas. Para este artículo, utilizaremos las configuraciones por defecto definidas en esta sección.



Configure las configuraciones siguientes:

• Retries – Ingrese la cantidad de veces que el conmutador intentará entrar en contacto con a un servidor de RADIUS antes de mover al servidor siguiente. El valor por defecto es 3.

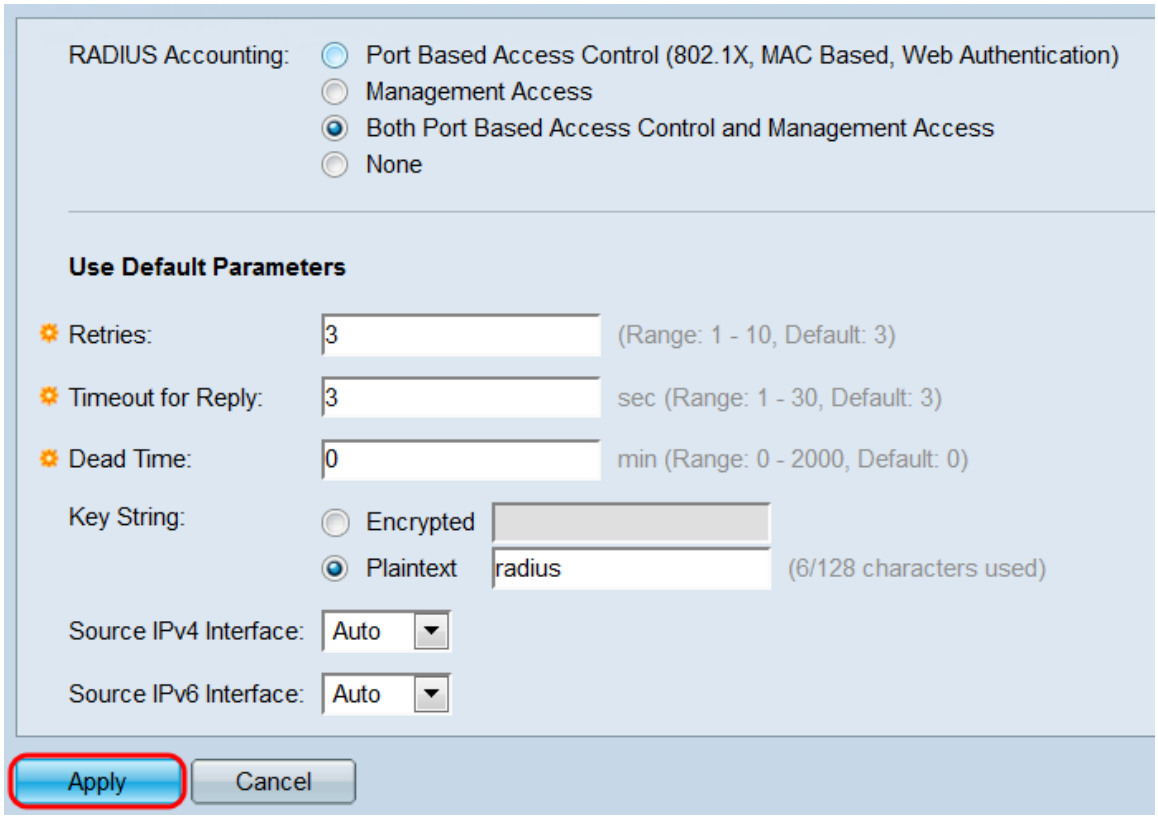
• Descanso para la contestación – Ingrese el número de segundos que el conmutador esperará una contestación del servidor de RADIUS antes de tomar otras medidas (que intentan otra vez o que dan para arriba). El valor por defecto es 3.

• Tiempo muerto – Ingrese el número de minutos que transcurran antes de que pasen un servidor de RADIUS no sensible encima para las peticiones del servicio. El valor por defecto es 0; este valor significa que el servidor no está desviado.

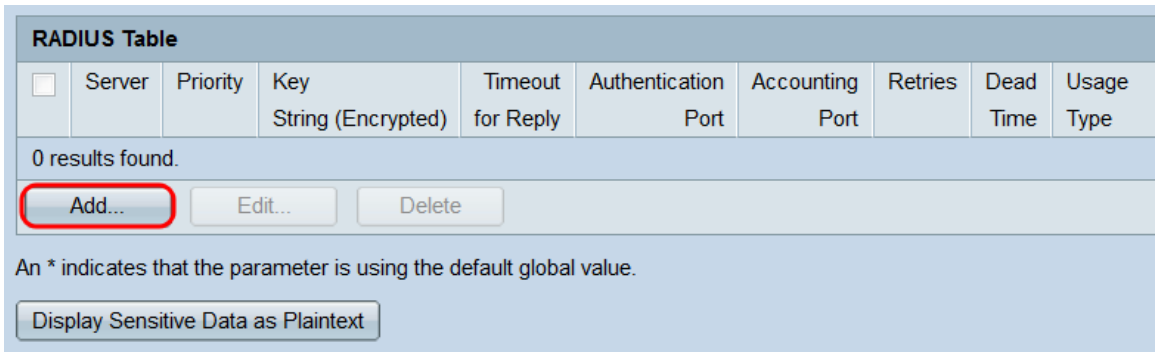
• Cadena dominante – Ingrese la clave secreta usada para autenticar entre el conmutador y el servidor de RADIUS. Si usted tiene una clave cifrada, ingresela con el botón de radio **cifrado**; si no, ingrese la clave del plaintext con el botón de radio del **Plaintext**.

• Interfaz de la fuente IPv4/IPv6 – Utilice estas listas desplegables para elegir que la interfaz de origen IPv4/IPv6 sea utilizada al comunicar con el servidor de RADIUS. El valor por defecto es auto, que utilizará la dirección IP de la fuente del valor por defecto definida en la interfaz saliente.

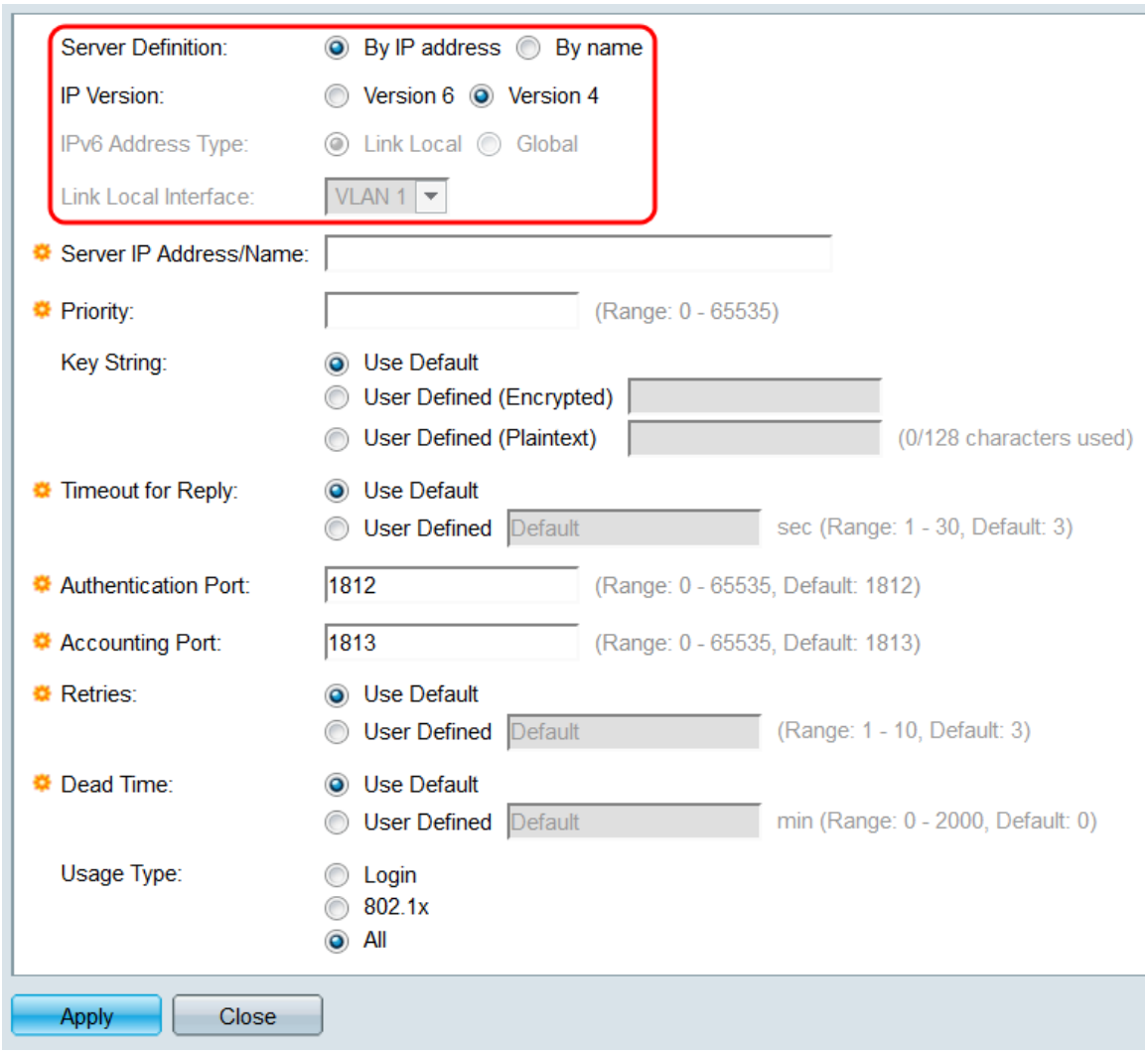
Paso 4. El tecleo **se aplica**. Las configuraciones por defecto serán aplicadas.



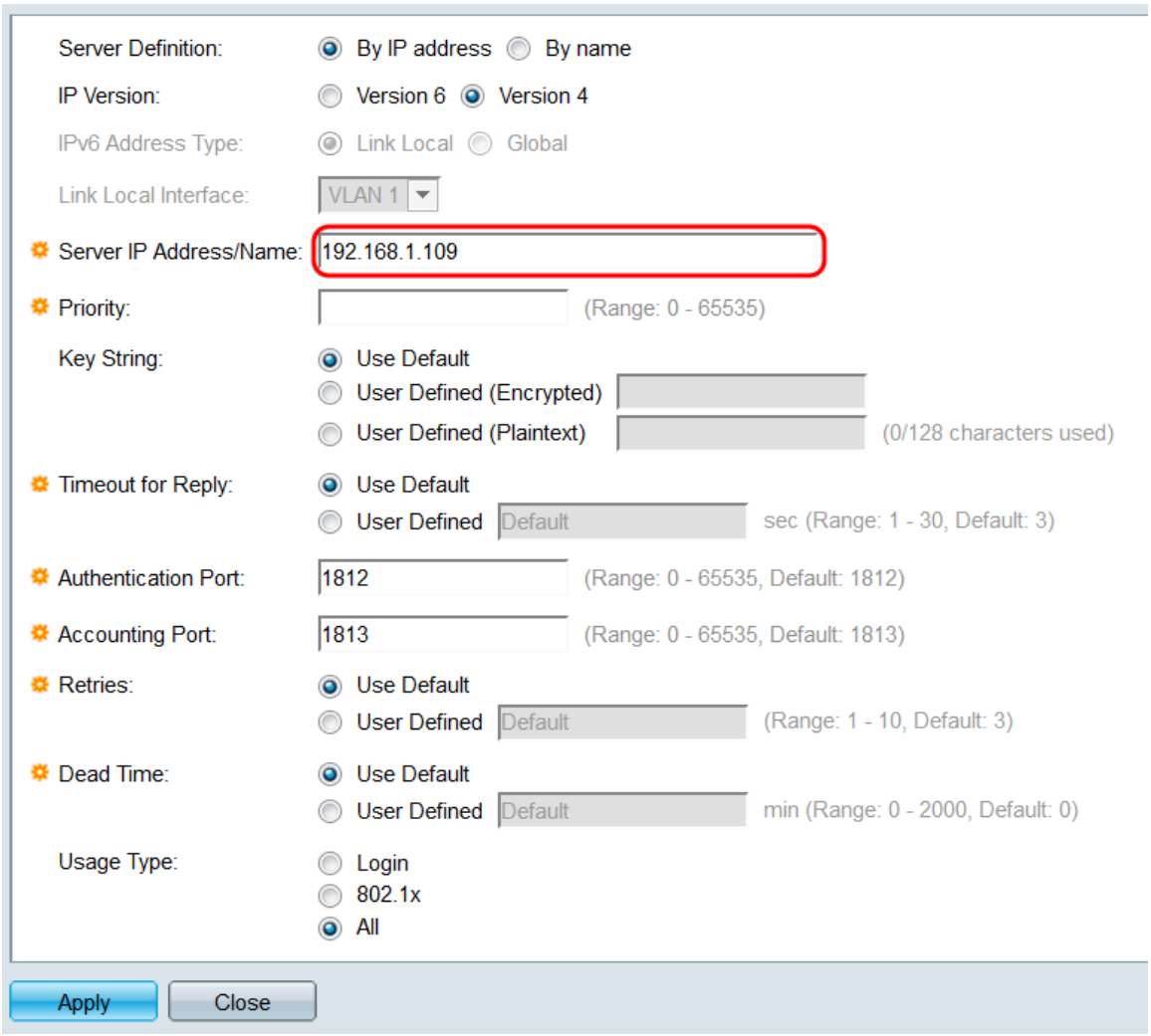
Paso 5. *La tabla RADIUS* mostrará las entradas del servidor de RADIUS configuradas actualmente en el conmutador. Para agregar una nueva entrada, haga clic el botón del **agregar…**. La ventana del *servidor de RADIUS del agregar* se abrirá.



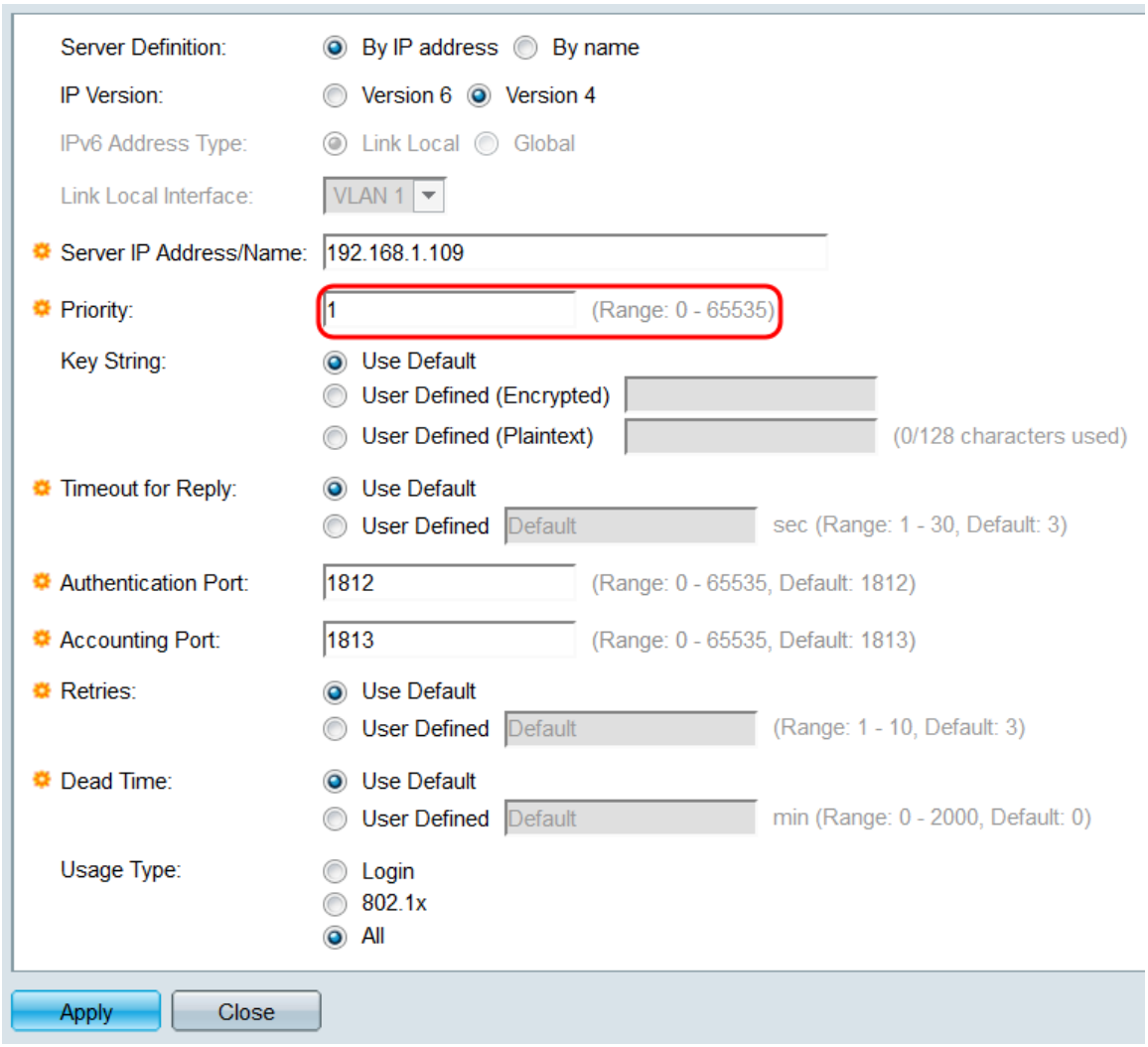
Paso 6. En el campo de *definición del servidor*, elija si entrar en contacto con al servidor de RADIUS **por la dirección IP** o **por nombre** (hostname). Si usted seleccionó **por la dirección IP** , seleccione para utilizar el IPv6 (**versión 6)** o IPv4 (**versión 4)**. Si usted seleccionó la **versión 6**, utilice la *interfaz local del tipo de dirección* y del *link del IPv6* para especificar el direccionamiento del IPv6 que será utilizado.



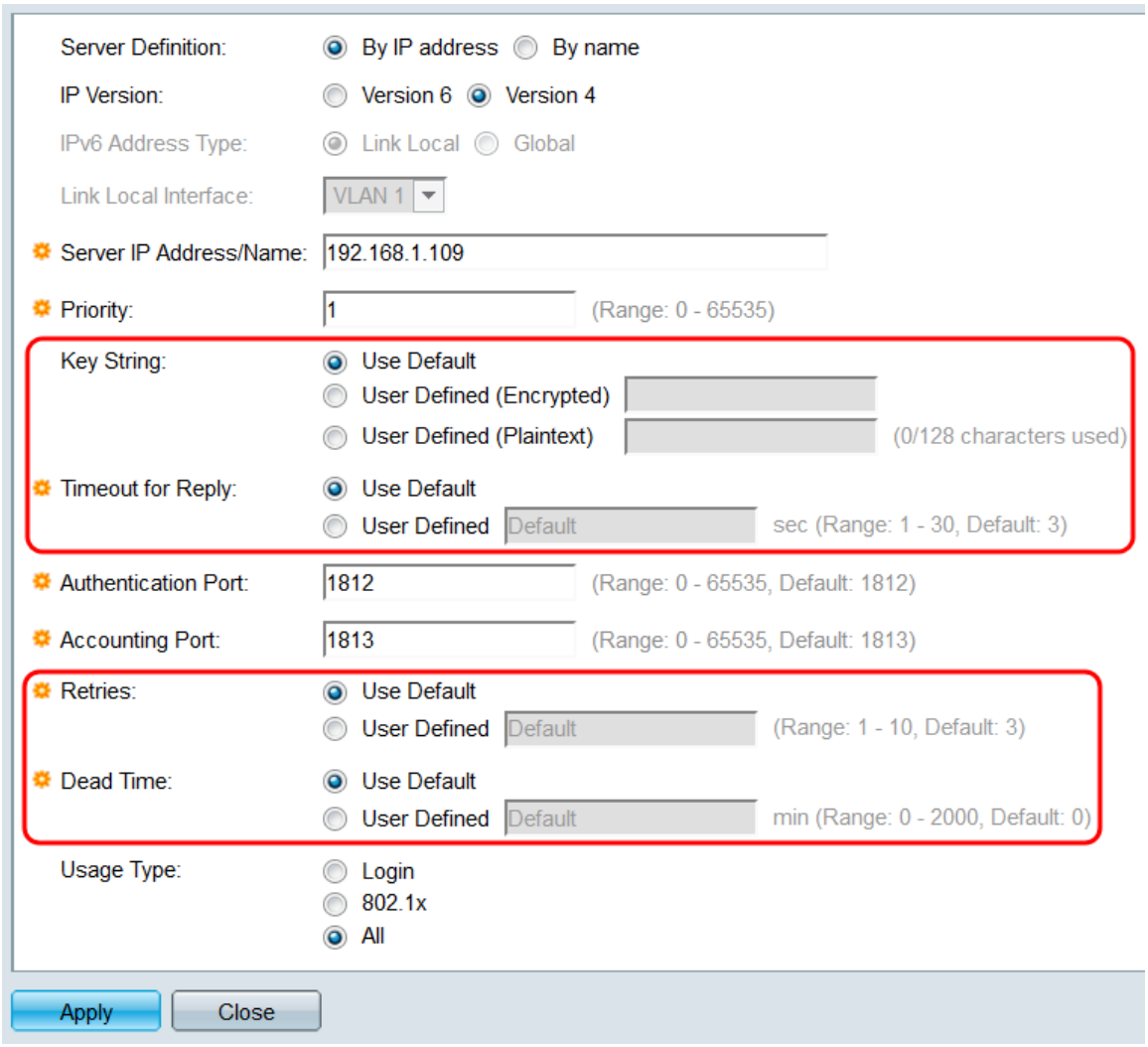
Paso 7. En el *IP address/el campo de nombre del servidor*, ingrese el IP address o el hostname del servidor de RADIUS.



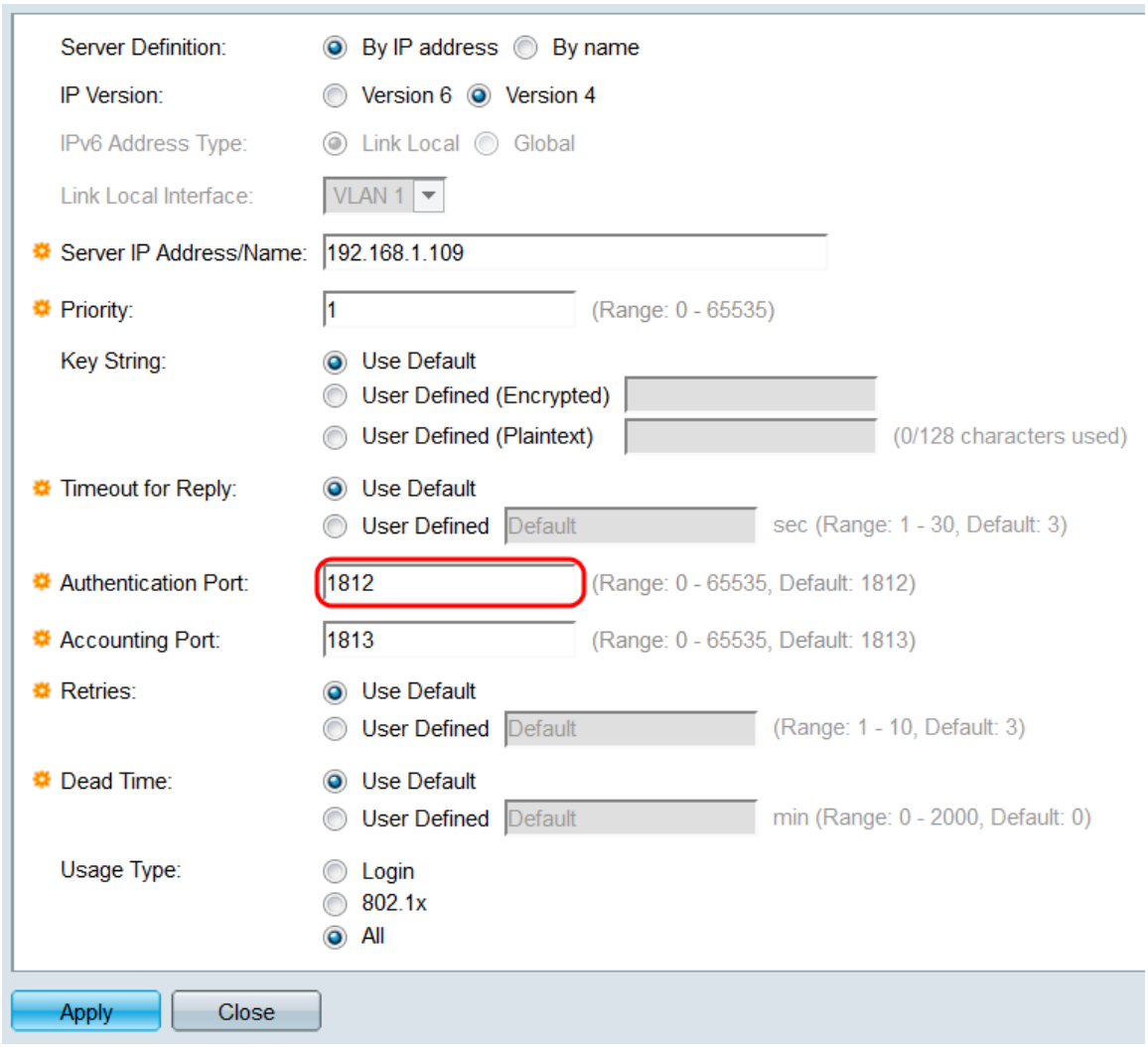
Paso 8. En el *campo de prioridad*, ingrese la prioridad que usted quiere asignar a este servidor; el conmutador intentará entrar en contacto con el servidor con la prioridad más alta y continuar abajo de la lista hasta que encuentre un servidor responsivo. El rango es 0 – 65535, con 0 siendo la prioridad más alta.



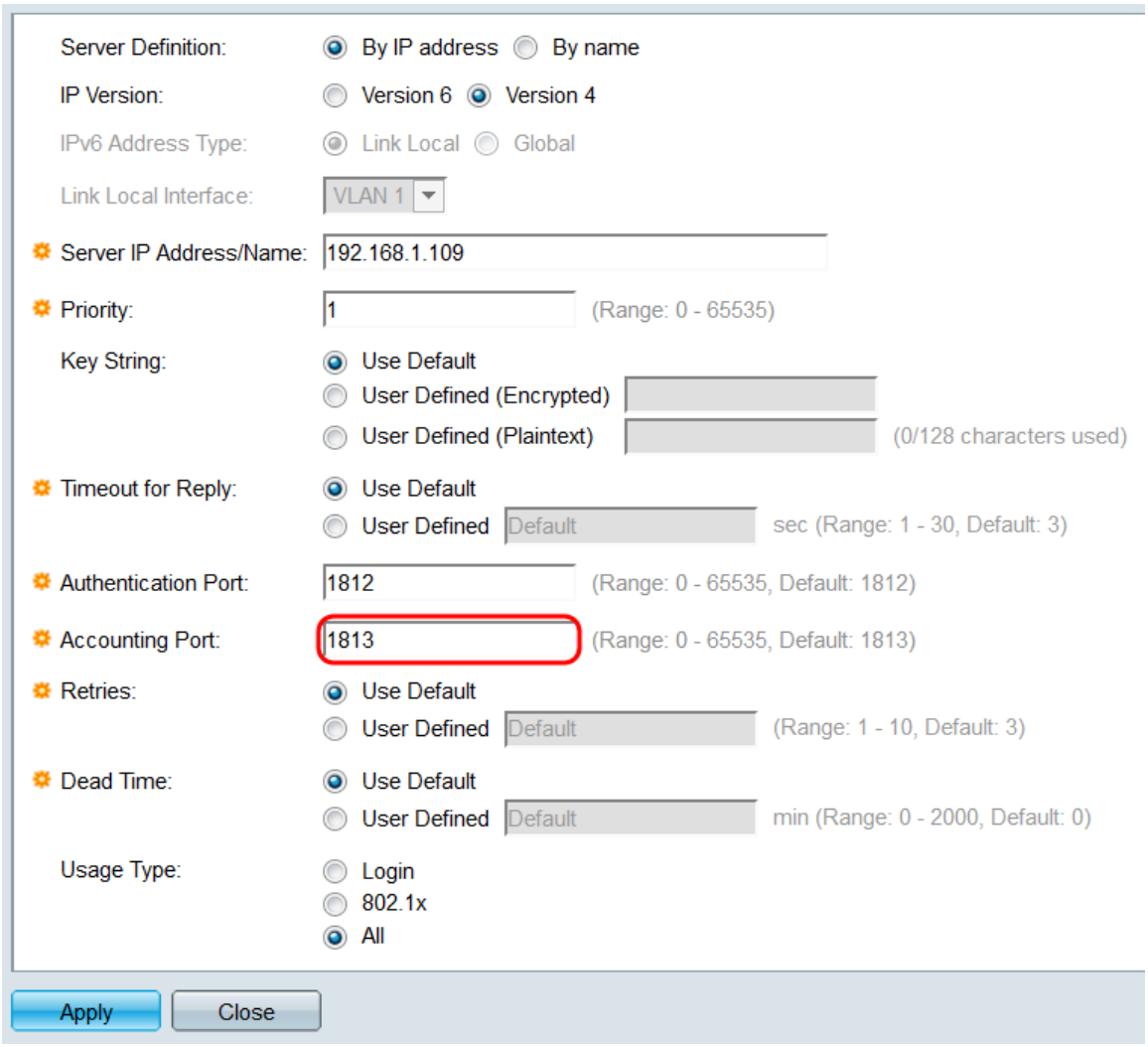
Paso 9. Seleccione el botón de radio del **valor por defecto del uso** en la *cadena dominante*, *descanso para que los* campos de la *contestación*, del *Retries*, y del *tiempo muerto* utilicen las configuraciones configuradas previamente en la página *RADIUS*. Usted puede también seleccionar los botones de radio **definidos por el usario** para configurar las configuraciones que son diferentes de los valores por defecto; si usted hace esto, estas configuraciones serán utilizadas solamente para este servidor de RADIUS específico.



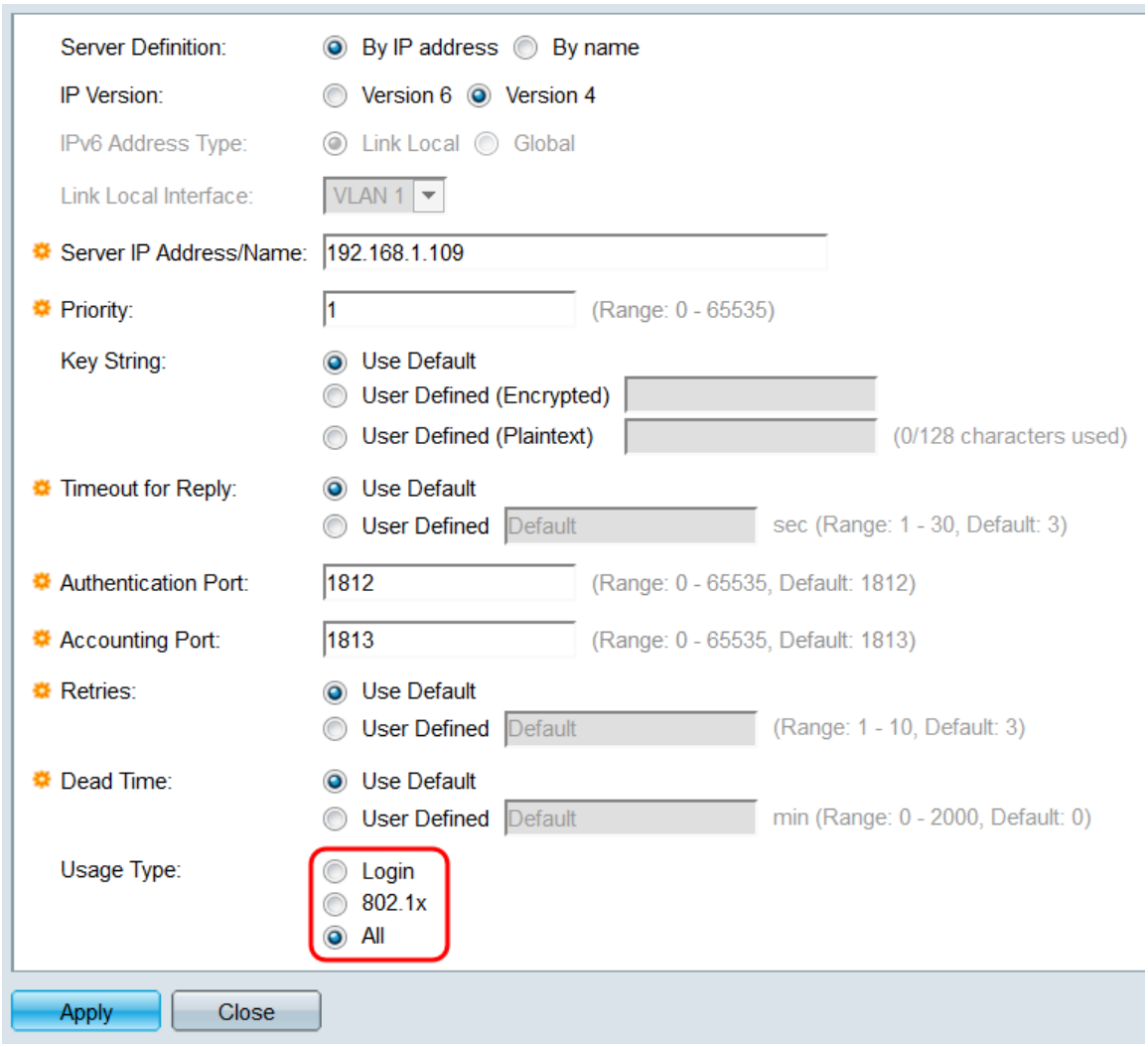
Paso 10. En el campo de *puerto de autenticación*, especifique el puerto que será utilizado para la comunicación de la autenticación con el servidor de RADIUS. Se recomienda que esto esté dejada en el puerto predeterminado, 1812.



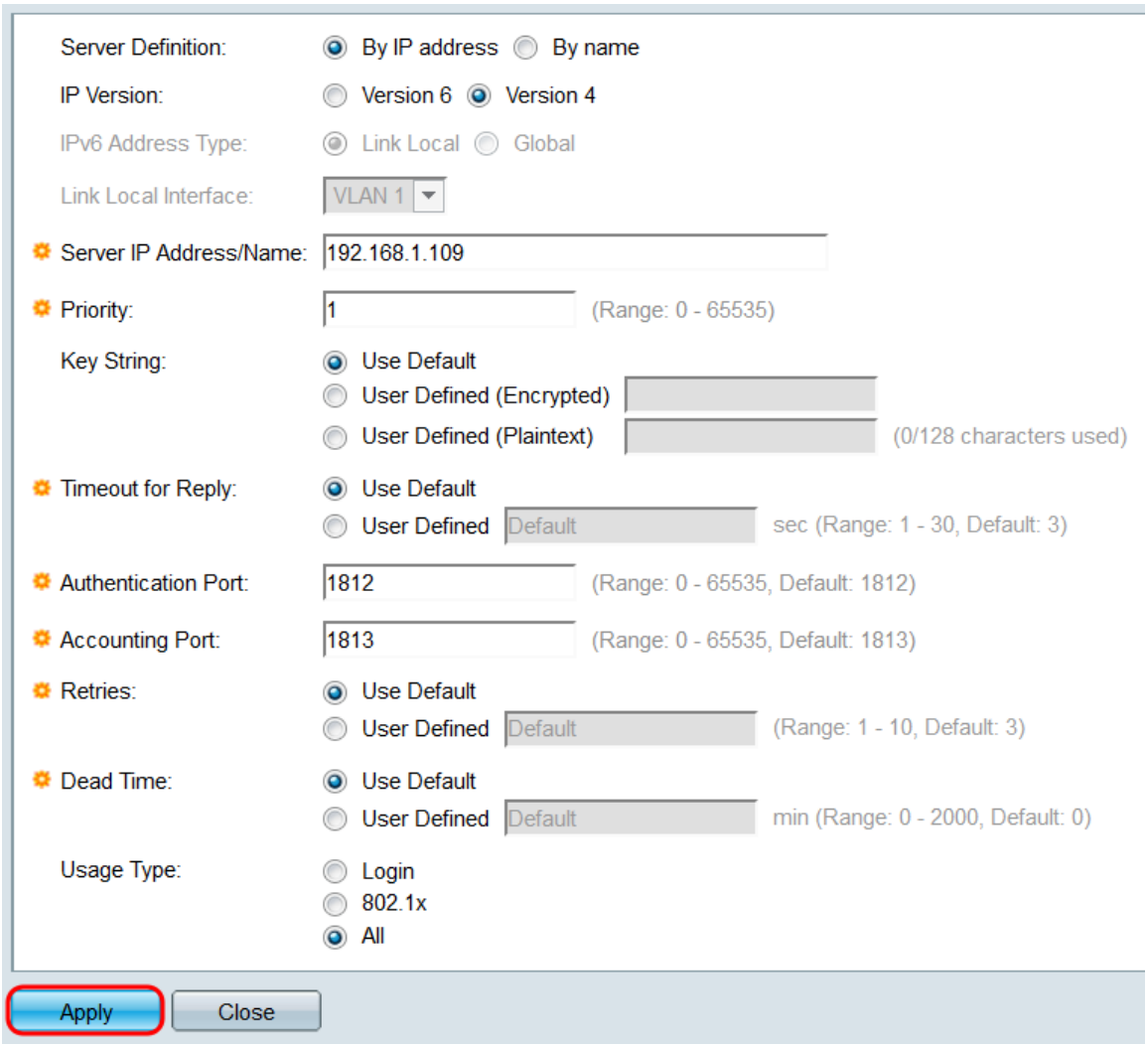
Paso 11. En el campo de *puerto de las estadísticas*, especifique el puerto que será utilizado para la comunicación que considera con el servidor de RADIUS. Se recomienda que esto esté dejada en el puerto predeterminado, 1813.



Paso 12. En el *tipo* campo del *uso*, seleccione para lo que utilizarán el servidor de RADIUS. Al configurar el 802.1x, seleccione el **802.1x** o **todos los** botones de radio para utilizar al servidor de RADIUS para la autenticación del puerto del 802.1x.

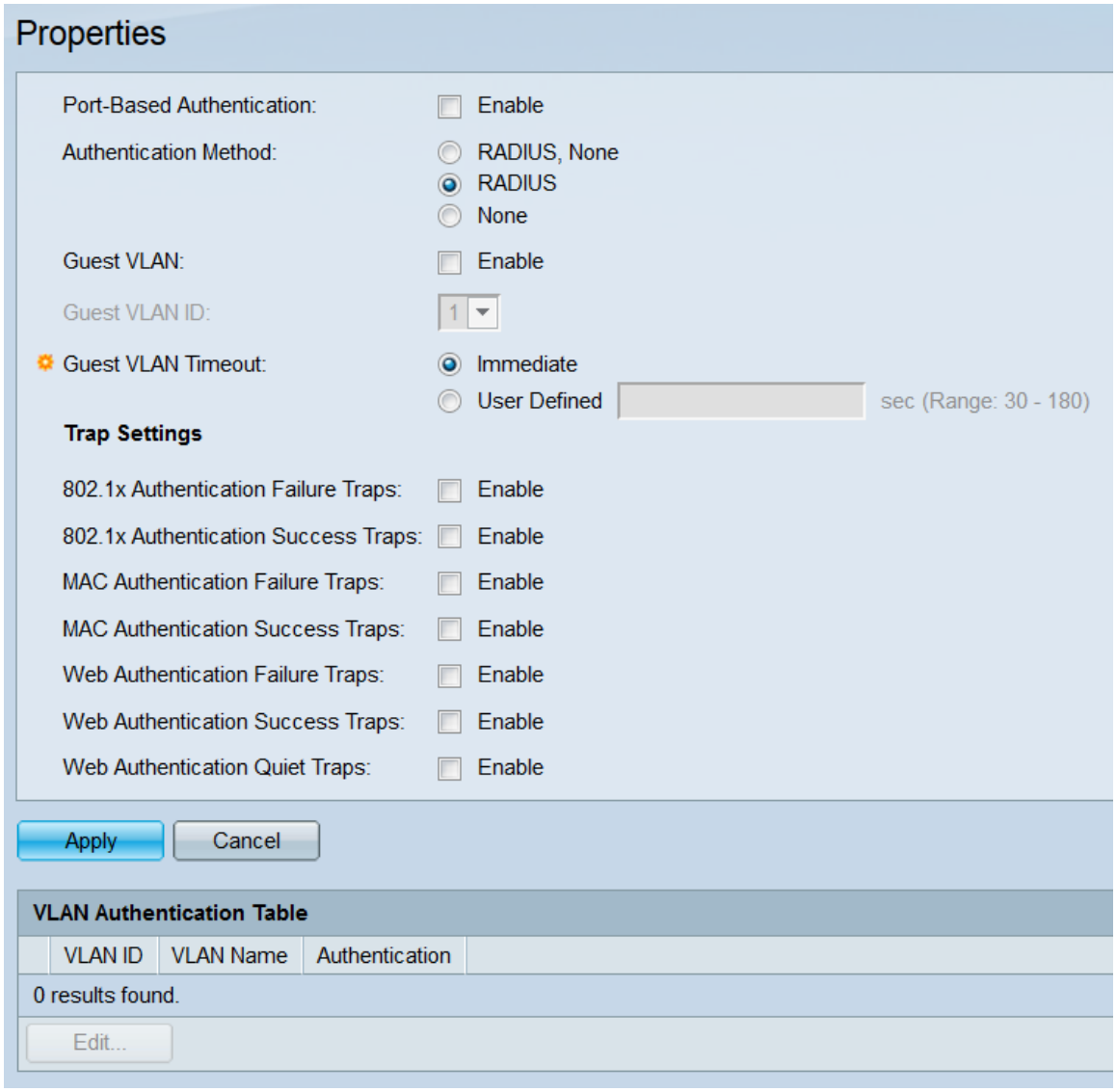


Paso 13. Haga clic en Apply (Aplicar). El servidor será agregado a la *tabla RADIUS*. Para activar puerto-basó la autenticación del 802.1x, continúa por favor a la siguiente sección.

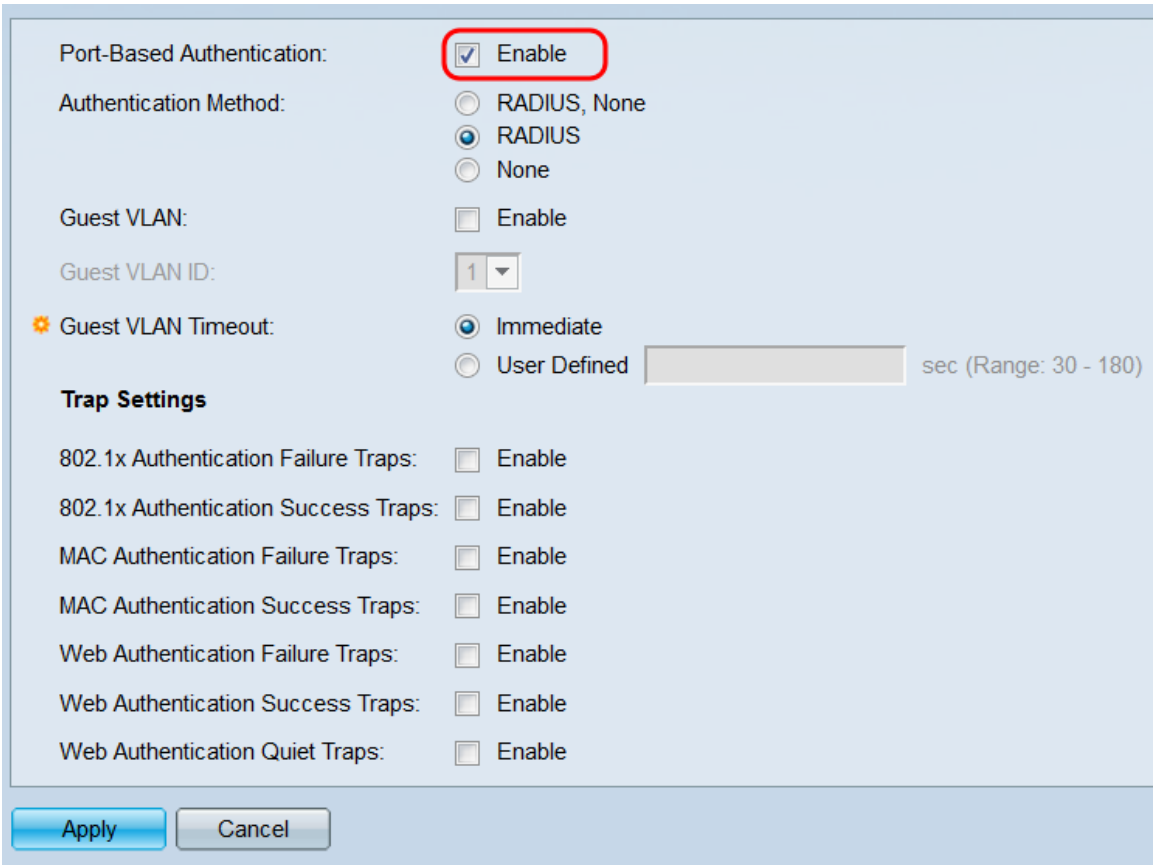


La activación Puerto-basó la autenticación

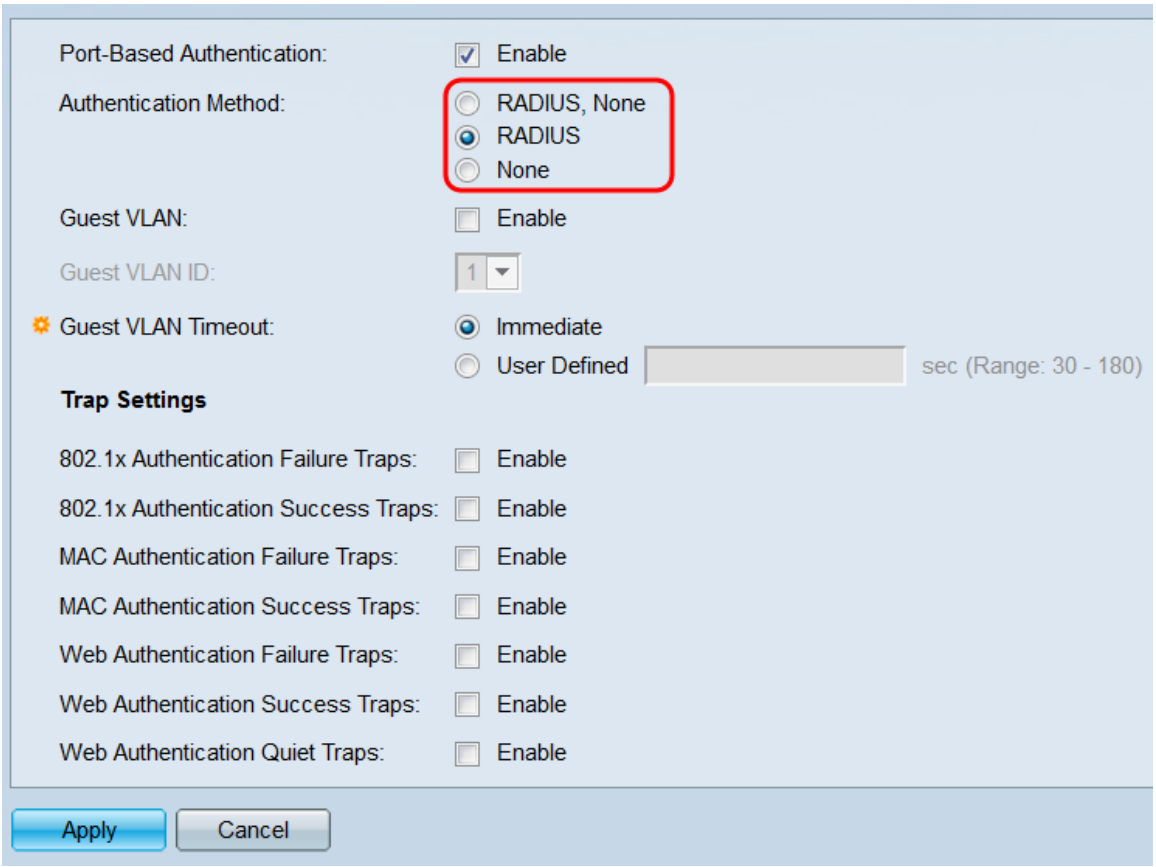
Paso 1. En la utilidad de configuración de la red, vaya a la **Seguridad > a la autenticación 802.1X/MAC/Web > a las propiedades**. La página de las *propiedades* se abre.



Paso 2. En el campo Puerto-*basado de la autenticación*, controle el checkbox del **permiso** para activar la autenticación puerto-basada. Esto se activa como opción predeterminada.



Paso 3. En el campo del *método de autenticación*, elija un botón de radio para determinar cómo la autenticación puerto-basada trabajará.



Las opciones son:

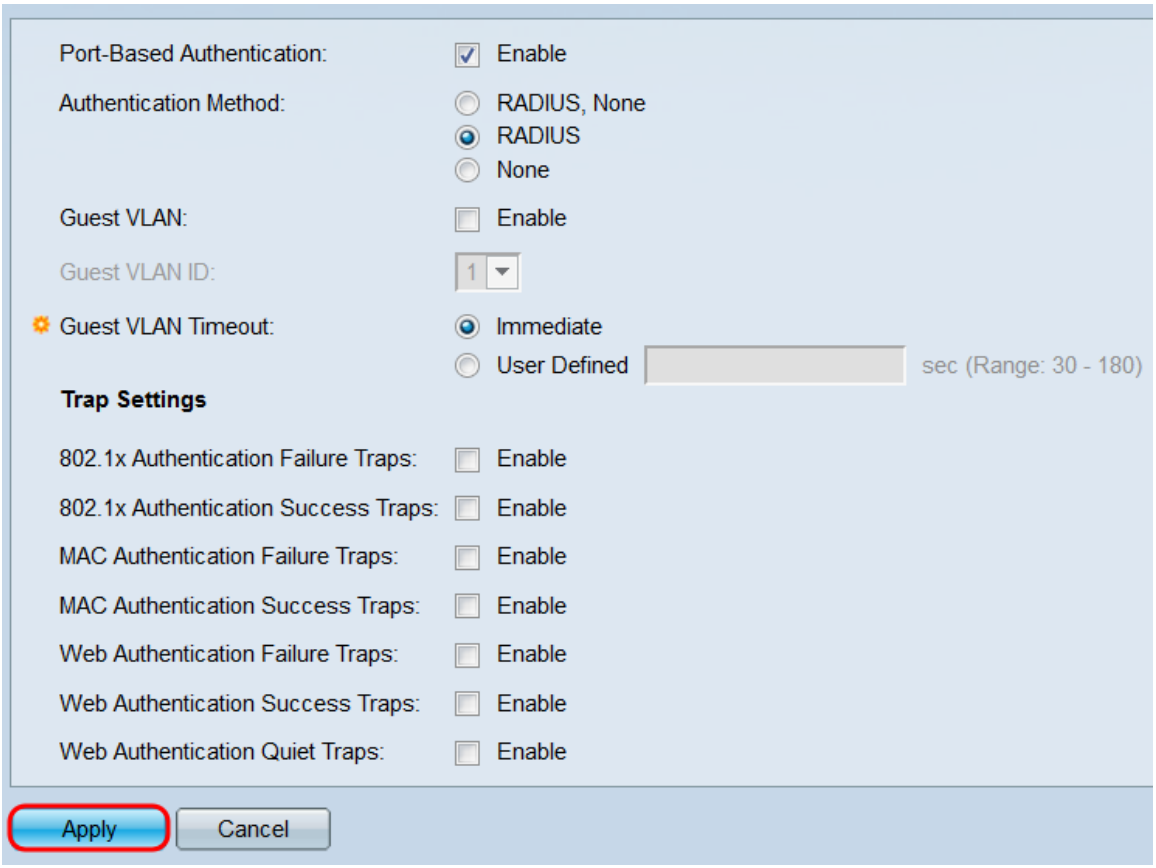
• RADIUS, ninguno – El conmutador intentará entrar en contacto con los servidores RADIUS definido en la página *RADIUS*. Si no se recibe ninguna respuesta de los

servidores, después no se realiza ninguna autenticación y se permite la sesión. Si el servidor es responsivo, y las credenciales son incorrectas, después se niega la sesión.

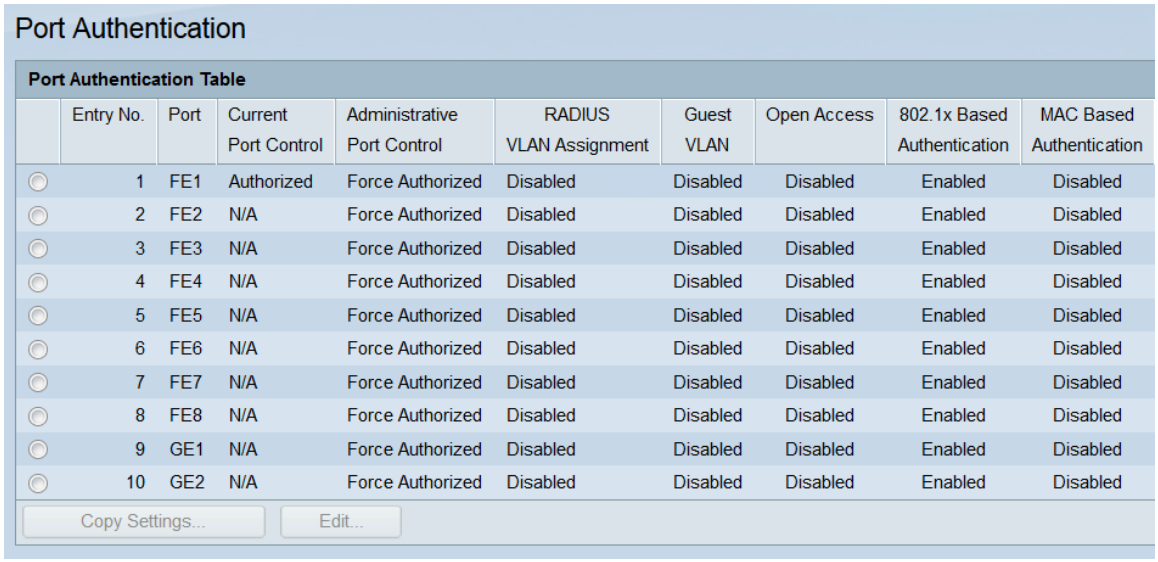
• RADIUS – El conmutador intentará entrar en contacto con los servidores RADIUS definido en la página *RADIUS*. Si no se recibe ninguna respuesta de los servidores, se niega la sesión. Para la puesta en práctica más segura del 802.1x, se recomienda esta opción.

• Ninguno – No se realiza ninguna autenticación. Todas las sesiones serán permitidas. Esta opción no ejecutará el 802.1x.

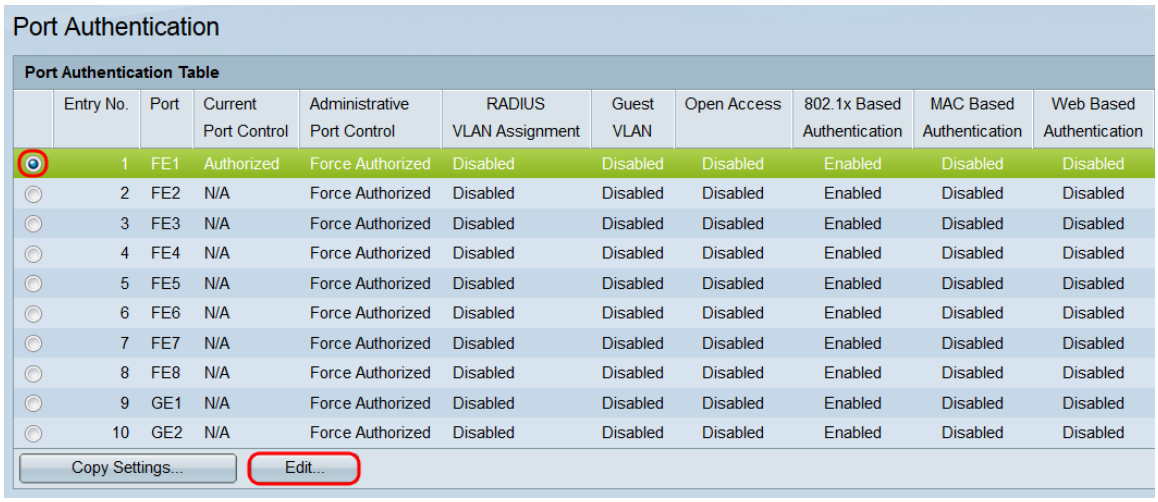
Paso 4. El tecleo **se aplica**.



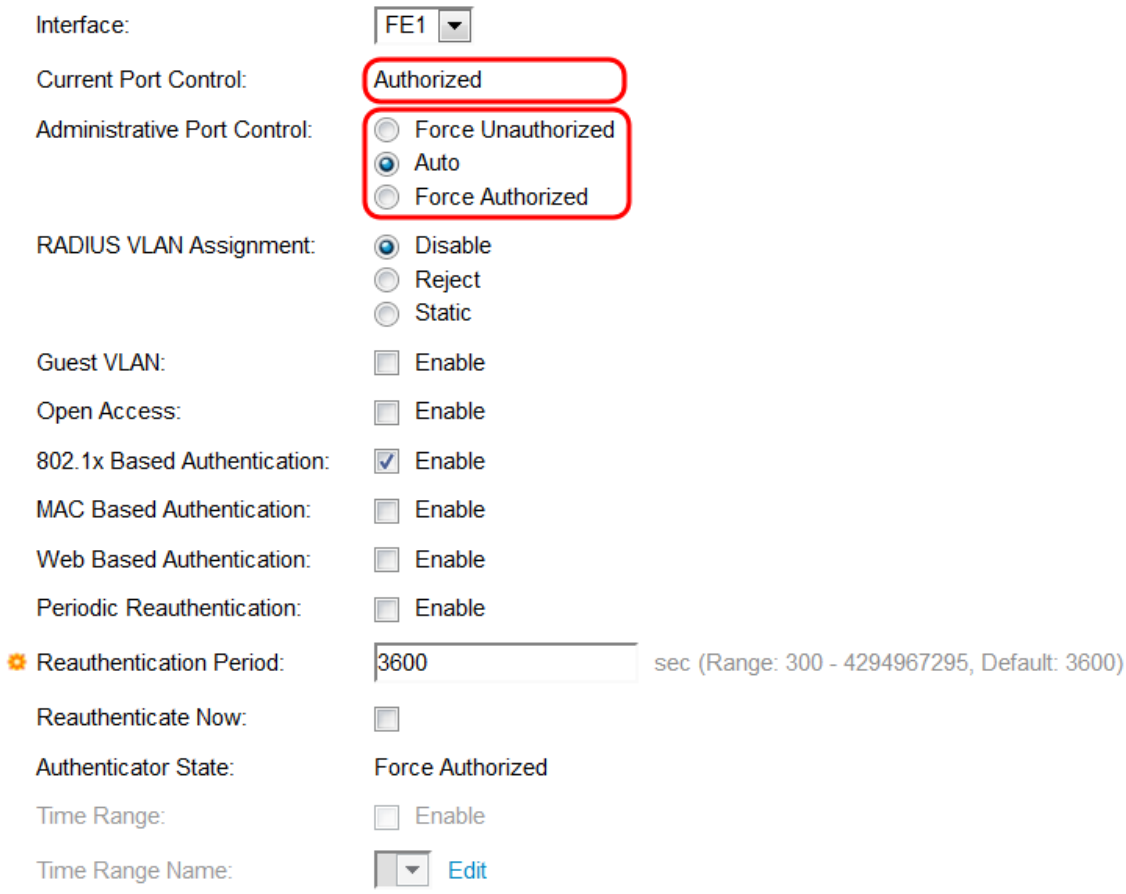
Paso 5. Navegue a la **Seguridad > a la autenticación 802.1X/MAC/Web > a la autenticación del puerto**. La página de la *autenticación del puerto* se abre.



Paso 6. Seleccione el puerto que usted quiere configurar seleccionando su botón de radio en la *tabla de la autenticación del puerto* y haciendo clic el botón del **corregir…**. *El puerto del corregir ventana Authentication (Autenticación)* se abre.



Paso 7. En el *Campo de control administrativo del puerto*, elija un botón de radio para determinar cómo el puerto autorizará las sesiones. *El Campo de control actual del puerto* visualiza el estado actual de la autorización del puerto seleccionado.



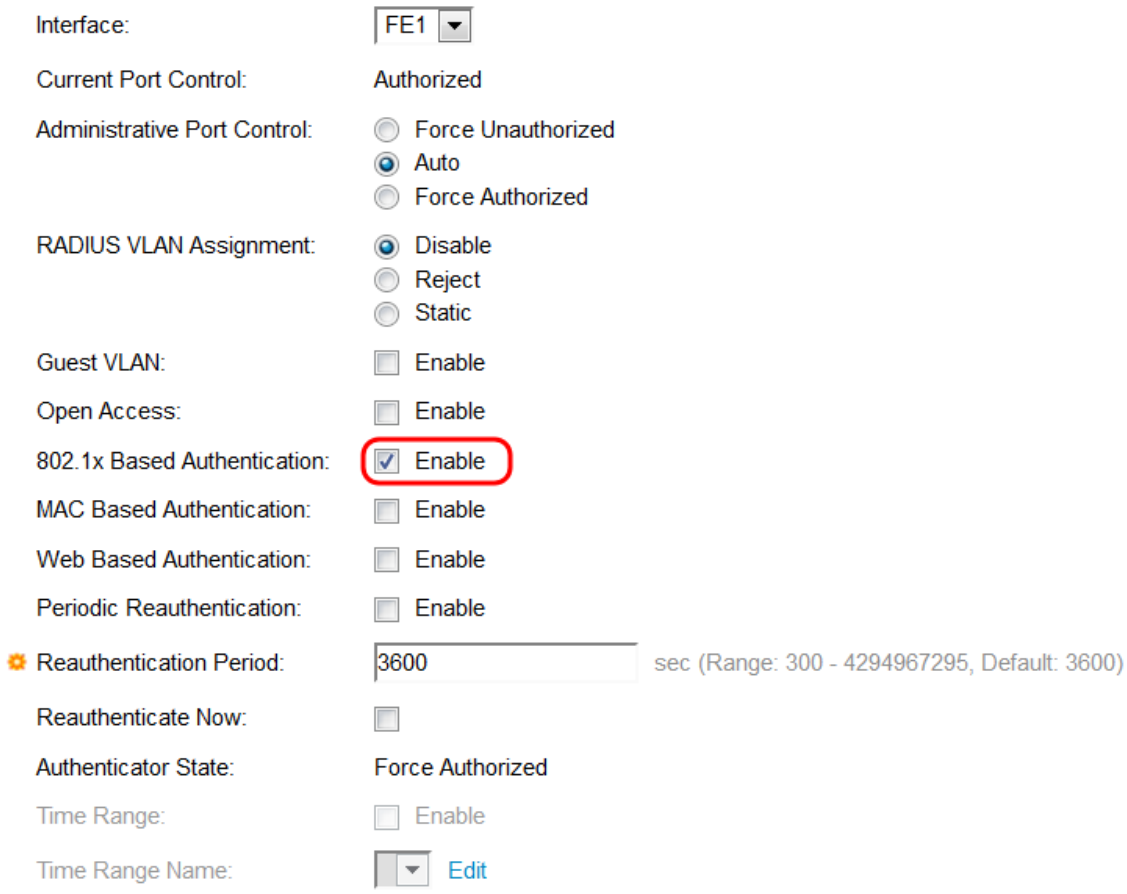
Las opciones son:

• Fuerza desautorizada – Se traslada el interfaz a un estado desautorizado. El dispositivo no proporciona a la autenticación a ninguna clientes conectada con este puerto, y niega el acceso.

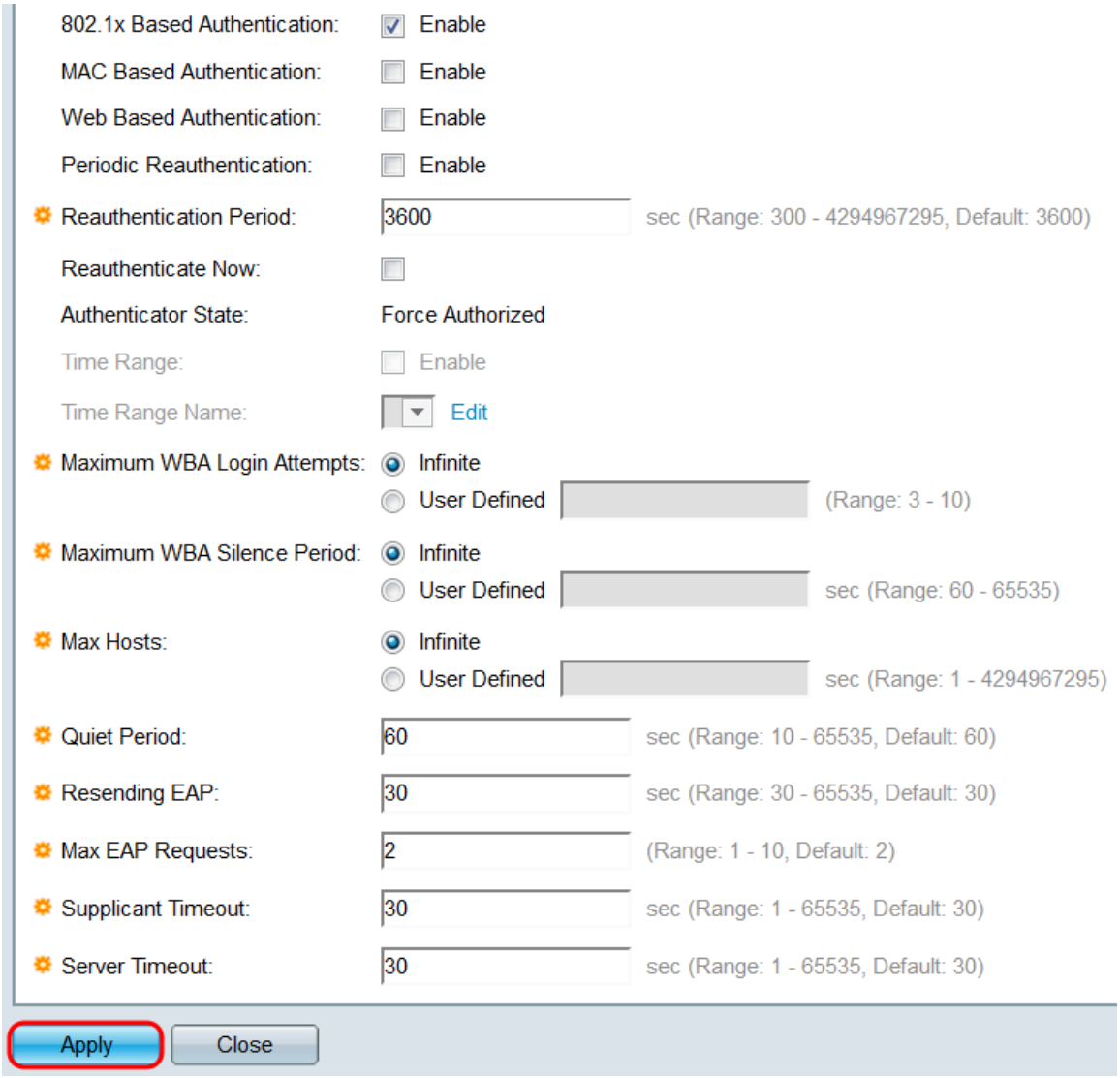
• Auto – Los permisos puerto-basaron la autenticación para el puerto seleccionado. Mueve el interfaz entre autorizado y desautorizado dependiendo del resultado del procedimiento de autenticación. Elija esta opción para ejecutar el 802.1x.

• Fuerza autorizada – Se traslada el interfaz a un estado autorizado. El dispositivo proporcionará al acceso a cualquier cliente que conecte con este puerto sin la autenticación.

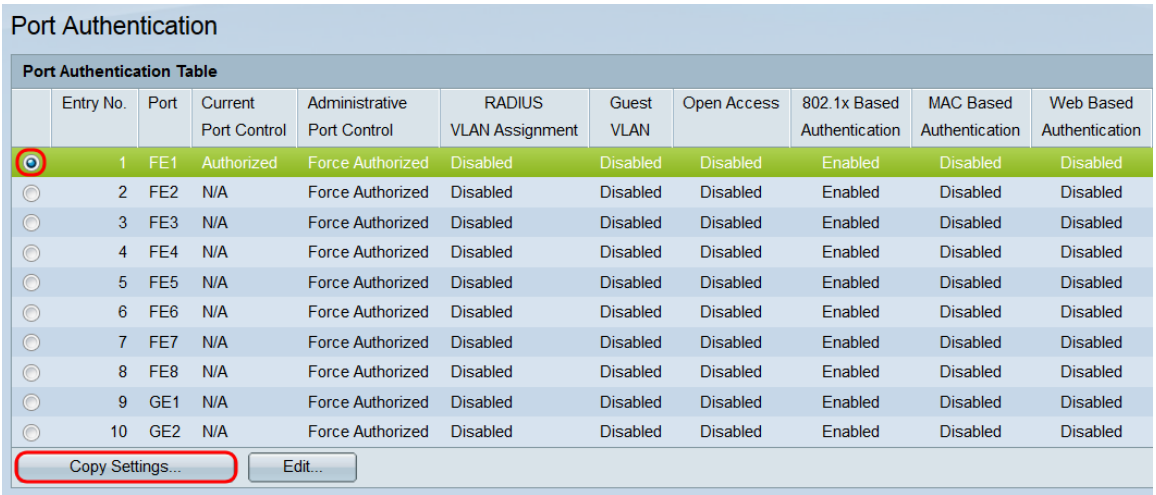
Paso 8. Controle el checkbox del **permiso** en el campo *basado 802.1x de la autenticación* para activar la autenticación del 802.1x para el puerto seleccionado.



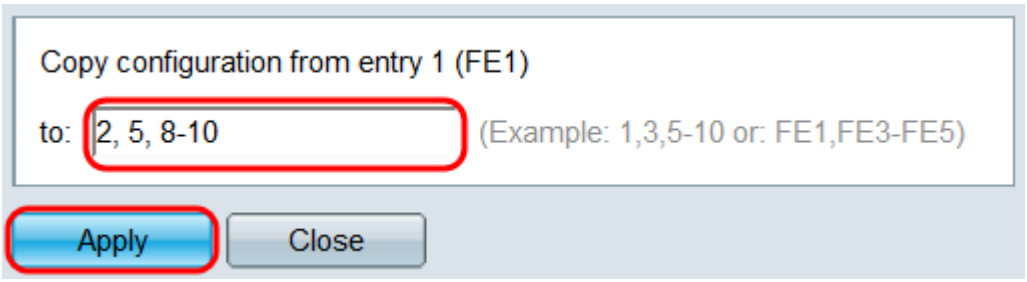
Paso 9. El tecleo **se aplica**. El puerto debe ahora ser de configuración completa para la autenticación puerto-basada 802.1x, y está listo para comenzar a autenticar a cualquier cliente que conecte con ella. Utilice el campo del *interfaz* para seleccionar un diverso puerto configurar sin volver a la página de la *autenticación del puerto*.



Paso 10. Si usted quiere copiar rápidamente las configuraciones de un puerto a otro puerto o rango de puertos, haga clic el botón de radio del puerto que usted quiere copiar en la *tabla de la autenticación del puerto* y hacer clic el botón de las **configuraciones de la copia…** . *La ventana de configuración de la copia* se abre.



Paso 11. En el campo de texto, ingrese el puerto o los puertos (separados por las comas) que usted quiere copiar las configuraciones a. Usted puede también especificar un rango de puertos. Entonces, el tecleo **se aplica** para copiar las configuraciones.


Copy configuration from entry 1 (FE1)
to:
2, 5, 8-10
(Example: 1,3,5-10 or: FE1,FE3-FE5)
Apply
Close