Authentifizierter und zeitbasierter Netzwerkzugriff mit 802.1x

802.1x ist ein IEEE-Standard für die portabhängige Netzwerkzugriffskontrolle. Cisco Small Business-Switches der Serie 300 unterstützen 802.1x für eine höhere Netzwerksicherheit. In einem 802.1x-fähigen Netzwerk fordert ein Benutzergerät wie ein Laptop oder ein IP-Telefon Port-Zugriff auf den direkt verbundenen Switch an. Der Switch erhält die Benutzer-ID und das Passwort des Benutzers (oder Geräts) und leitet diese zur Authentifizierung an einen RADIUS-Server weiter. Der Switch erteilt nur dann Port-Zugriff, wenn die Benutzerauthentifizierung erfolgreich ist. Dieser authentifizierte LAN-Zugriff erhöht die Netzwerksicherheit.

Beschriebene Produkte

In diesem Smart Tip wird die Verwendung der auf 802.1x basierenden Authentifizierung bei einem Cisco Small Business Managed Switch der Serie 300 (Modell SF300-48P) mit mehreren Ports mit und ohne PoE (Power over Ethernet) beschrieben. Informationen zu anderen Cisco Managed Switches der Serie 300 finden Sie unter http://www.cisco.com/go/300switches.

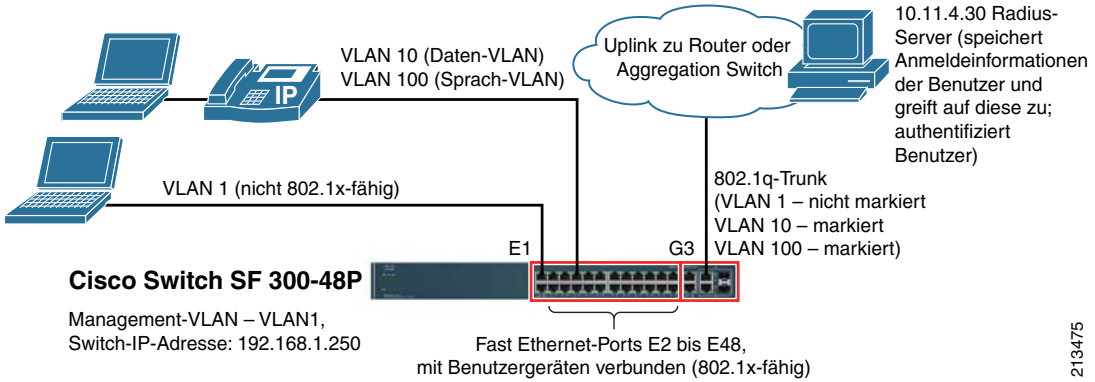
Aufbau 802.1x-fähiger Netzwerke

Ein wie in Abbildung 1 dargestelltes Netzwerk mit auf 802.1x basierender Authentifizierung beinhaltet folgende Hauptkomponenten:

- Laptops/IP-Telefone (oder andere ähnliche Endbenutzergeräte, die auf 802.1x basierenden Zugriff auf ein Netzwerk anfordern können)
- Ein Switch, der den Benutzer über einen RADIUS-Server authentifiziert und Netzwerkzugriff nur bei erfolgreicher Authentifizierung erteilt
- Ein RADIUS-Server für die Benutzerauthentifizierung

Wenn die 802.1x-Authentifizierung in einem LAN aktiviert ist, wird sie in der Regel für alle Switch-Ports aktiviert, die mit Endbenutzergeräten oder anderen Geräten, die einen authentifizierten Port-Zugriff erfordern, verbunden werden.

Abbildung 1 Authentifizierter Netzwerkzugriff mit 802.1x



Authentifizierung

Zur Benutzerauthentifizierung greift der RADIUS-Server auf eine Benutzerdatenbank zu, die Informationen wie Benutzer-ID und Passwort sowie weitere optionale Informationen enthält. Diese werden bei erfolgreicher Authentifizierung an den Switch weitergeleitet. Die Datenbank kann in den RADIUS-Server integriert werden, oder es wird eine externe Datenbank wie Active Directory verwendet.

Zur Authentifizierung konfigurierte Ports

Die auf 802.1x basierende Authentifizierung eignet sich in erster Linie für Endbenutzergeräte wie Laptops oder IP-Telefone, bei denen es sich sicherheitstechnisch um nicht vertrauenswürdige Geräte handelt. 802.1x wird deshalb nicht auf Ports konfiguriert, die mit Netzwerkgeräten wie Routern, Switches, Servern oder anderen vertrauenswürdigen Geräten verbunden sind. Eine Konfiguration erfolgt stattdessen auf Ports, die Benutzergeräte mit einem Access Switch oder auch – falls ein direkter Anschluss von Benutzergeräten möglich ist – mit einem Aggregation Switch verbinden.

Richtlinie für die Port-Authentifizierung

Zur Konfiguration des Cisco Small Business-Switch-Ports der Serie 300 kann eine der folgenden drei Richtlinien herangezogen werden. Diese legen fest, wie sich eine auf 802.1x basierende Authentifizierung auf den Port-Zugriff auswirkt, wenn mehrere Geräte an einen einzelnen Port angeschlossen werden können:

- Single – Nur ein autorisierter Host kann auf den Port zugreifen.
- Multiple host (802.1x) – Der Port unterstützt mehrere Hosts. Nur der erste Host muss nach 802.1x autorisiert werden. Bei erfolgreicher Autorisierung können nicht nur das authentifizierte Gerät, sondern auch alle anderen angeschlossenen Geräte ohne eine weitere Authentifizierung auf den Port zugreifen. Die Geräte können erst auf den Port zugreifen, wenn mindestens ein angeschlossenes Gerät erfolgreich authentifiziert wurde. Dies ist für die Implementierung von Geräten nützlich, die 802.1x nicht unterstützen.
- Multiple sessions – Mehrere Hosts können auf den Port zugreifen, jeder Host muss aber einzeln und separat authentifiziert werden.

Hinweis In Cisco SMART Designs wird für eine höhere Flexibilität und Sicherheit die Richtlinie für mehrere Sitzungen empfohlen. Die Richtlinie für mehrere Hosts kann zur Unterstützung von Geräten an einem Port verwendet werden, der eine 802.1 x-Authentifizierung nicht unterstützt.

Hinweis Der Cisco Small Business-Switch der Serie 300 kann so konfiguriert werden, dass ein Benutzer in das Gast-VLAN verschoben wird, wenn die 802.1x-Benutzerauthentifizierung fehlschlägt.

Überlegungen zum RADIUS-Server

Der Cisco Small Business-Switch der Serie 300 greift über das Management-VLAN auf den RADIUS-Server zu und verwendet dabei die dem Switch zugewiesene einzelne Management-IP-Adresse (als Layer 3-fähiger Switch unterstützt er auch mehrere IP-Schnittstellen). Dies impliziert, dass der Switch den RADIUS-Server über sein Management-VLAN erreichen kann. Wenn sich der RADIUS-Server auf einem anderen VLAN (nicht wie in Abbildung 1 angenommen) befindet, übernimmt normalerweise der WAN-Router das erforderliche Inter-VLAN-Routing.

Der WAN-Router terminiert das Management-VLAN. Bei Verwendung des werksseitig eingestellten Management-VLANs (VLAN 1) müssen die LAN-Switches so konfiguriert werden, dass sie das nicht markierte VLAN 1 gegebenenfalls zusammen mit anderen VLANs über ihre Trunk-Ports an den WAN-Router weiterleiten.

Authentifizieren von IP-Telefonen

IP-Telefone können ebenso wie PCs und Laptops 802.1x-authentifiziert werden. Cisco IP-Telefone sind 802.1x-fähig. Informationen zur Aktivierung der 802.1x-Authentifizierung auf dem IP-Telefon und zur Erstellung einer geeigneten Benutzer-ID für das IP-Telefon im RADIUS-Server finden Sie im Administratorhandbuch für das jeweilige IP-Telefon.

Zeitbasierte Authentifizierung

Mit dem Cisco Small Business-Switch der Serie 300 können Sie den Zugriff auf 802.1x-fähige Ports auf einen bestimmten Zeitraum beschränken. Hierzu wird ein absoluter Zeitraum wie 22. Februar 2010, 9 Uhr, bis 30. April 2023, 17 Uhr, angegeben. Benutzer sind dann jederzeit während des angegebenen Zeitraums zum authentifizierten Port-Zugriff berechtigt. Außerhalb dieses Zeitraums befinden sich die Ports im Zustand „Force Unauthorized“. Ein Zugriff auf die Ports ist dann nicht möglich, und es wird keine 802.1x-Authentifizierung initiiert.

Nach der Einrichtung eines absoluten Zeitraums können Sie diesen genauer definieren und einen sich wiederholenden Zeitraum hinzufügen. Durch einen sich wiederholenden Zeitraum wird der Benutzerzugriff weiter auf einen für jeden Wochentag spezifischen Start- und Endzeitpunkt eingeschränkt (Sie können für verschiedene Wochentage separate Zeiträume definieren).

Ports können verschiedenen Zeiträumen zugewiesen werden. Dies ist nützlich, wenn Mitarbeiter unterschiedliche Arbeitszeiten haben (oder zu unterschiedlichen Zeiten auf das Netzwerk zugreifen).

Dynamische VLAN-Zuordnung

Bei der dynamischen VLAN-Zuordnung (DVA) wird einem benutzerspezifischen VLAN nach erfolgreicher 802.1x-Authentifizierung dynamisch ein Port zugeordnet. Das VLAN des Benutzers muss im RADIUS-Benutzerprofil definiert werden. Wenn der Benutzer erfolgreich authentifiziert wurde, leitet der RADIUS-Server die VLAN-Informationen des Benutzers als Teil des Authentifizierungsverfahrens an

den Switch weiter. Der Switch fügt den Port dann als nicht markiertes (untagged) Mitglied dieses VLANs hinzu. Wenn verschiedene Benutzer abteilungsbedingt oder aufgrund anderer Kriterien separaten Daten-VLANs angehören, wird so die Benutzermobilität verbessert.

Der Cisco Small Business-Switch der Serie 300 unterstützt DVA, jedoch wird in diesem Dokument nicht auf die Konfiguration dieser Funktion eingegangen. Weitere Informationen dazu finden Sie im Administratorhandbuch unter der folgenden URL: http://www.cisco.com/en/US/docs/switches/lan/csbms/sf30x_sg30x/administration_guide/78-19308-01.pdf.

Tipps zur Konfiguration

Dieser Abschnitt enthält ein Beispiel für die 802.1x-Konfiguration eines Cisco Small Business-Switches der Serie 300. In dem Beispiel werden die Fast Ethernet-Ports eines Cisco Switches SF 300-48P von e2 bis e48 konfiguriert, um den authentifizierten Port-Zugriff über 802.1x zu ermöglichen.

Dieser Abschnitt bezieht sich auf die Konfiguration eines Access Switches in einer Cisco SMART Design-Topologie, wie sie in Abbildung 1 dargestellt ist.

Netzwerkanforderungen für diese Konfiguration

LAN-Anforderungen

1. Alle Switch-Ports eines Cisco Small Business-Switches der Serie 300 sind als Werkseinstellung dem nativen VLAN 1 zugeordnet. In der Praxis müssen häufig weitere separate VLANs für den Daten- und Sprachdatenverkehr eingerichtet werden. In diesem Konfigurationsbeispiel werden VLAN 10 als das Daten-VLAN und VLAN 100 als das Sprach-VLAN verwendet.

   Als Beispiel wird VLAN 1 ein einzelner Port (e1) zugeordnet, der als dedizierter Management-Port dient. In der Praxis kann jedoch auch VLAN 10 (Daten-VLAN) als das Management-VLAN verwendet werden. Die Verwendung dedizierter Management-Ports ist jedoch optional.
2. Alle diese VLANs (VLANs 10, 100 und 1) werden durch den WAN-Router terminiert.
3. Für die Konfiguration eines Ports über einen Cisco Switch der Serie 300 stehen folgende drei Möglichkeiten zur Auswahl:
   - Access port – Der Port kann einem einzelnen VLAN, der PVID (Port VLAN ID), zugeordnet werden. Ein Zugriffs-Port leitet alle eingehenden Datenpakete über den Port in die PVID weiter. Da nur ein einzelnes VLAN unterstützt wird, eignet sich diese Alternative nicht bei der Verwendung separater Daten- und Sprachdaten-VLANs.
   - Trunk port – Der Port bietet Unterstützung für eine einzelne PVID und ein oder mehrere gekapselte (markierte) 802.1q-VLANs. Wie in Tabelle 1 dargestellt, stützt sich dieses Design auf Trunk-Ports.
   - General port – Dieser Port unterstützt mehrere markierte und nicht markierte (tagged /untagged) VLANs, und nicht markierter Datenverkehr wird je nach Quell-MAC-Adresse an VLANs weitergeleitet.

Bei dieser Konfiguration wird davon ausgegangen, dass der Access Switch wie in Tabelle 1 dargestellt konfiguriert ist. Die tatsächlich verwendeten VLAN-Nummern und -Ports können bei einer Implementierung je nach den spezifischen Anforderungen hiervon abweichen (siehe Abbildung 1).

Tabelle 1 Port-Konfigurationen für dieses Beispiel

	Port-Nummer	Port-Typ	PVID (Port VLAN ID)	Tagged (markierte) VLANs	Ausgeschlossene VLANs
Spezifische Switch-Management-Schnittstelle (optional)	e1	Trunk	VLAN 1		10, 100
Mit Laptops/IP-Telefonen von Benutzern verbundene Ports	e2 bis e48	Trunk	VLAN 10 (Daten-VLAN)	VLAN 100 (Sprach-VLAN)	1
Upstream-Port	G3 (auch G1, G2, G4)	Trunk	VLAN 1	VLANs 10, 100	1

4. Bei dem Switch ist RSTP (Rapid Spanning Tree Protocol) aktiviert, und er kann unter Verwendung seiner VLANs Datenverkehr über das LAN weiterleiten.

Konfiguration des Aggregation Switches

Bei dieser Konfiguration wird davon ausgegangen, dass der Aggregation Switch wie in Tabelle 2 dargestellt konfiguriert ist.

Tabelle 2 Konfiguration des Aggregation Switches

	Mit dem Cisco Switch der Serie 300 verbundener Port	Mit dem WAN-Router verbundener Port
VLAN 1	Nicht markiert (PVID)	Nicht markiert (PVID)
VLAN 10	Markiert	Markiert
VLAN 100	Markiert	Markiert

Hinweis Vergewissern Sie sich, dass der Aggregation Switch für die Weiterleitung des nicht gekennzeichneten VLANs 1 konfiguriert ist (wenn beispielsweise ein Cisco Catalyst-Switch verwendet wird, muss das nicht markierte VLAN in die VLANs aufgenommen werden, damit es mit einem Befehl wie **switchport trunk allowed vlan 1,10,100** über den Trunk-Port geleitet werden kann).

Konfigurationsanforderungen für den WAN-Router

Es wird davon ausgegangen, dass der WAN-Router die VLANs wie in Tabelle 3 dargestellt terminiert.

Tabelle 3 VLAN-Terminierung durch den WAN-Router

	Port-Verbindung des Routers mit dem Cisco Switch der Serie 300	
	VLAN-Schnittstellentyp	IP-Adresse (Standard-Gateway für das Subnetz)
VLAN 1	Natives VLAN (nicht markiert)	192.168.1.1
VLAN 10	Markiert	10.1.20.1
VLAN 100	Markiert	10.1.100.1

Konfigurationsanforderungen für den RADIUS-Server

1. Vergewissern Sie sich, dass der RADIUS-Server für die Annahme von RADIUS-Authentifizierungsanforderungen für den spezifischen Switch konfiguriert ist. Dies bedeutet, dass die Switch-IP-Adresse und der Authentifizierungscode (gemeinsames Passwort) im RADIUS-Server angegeben sein müssen. Auf dem RADIUS-Server müssen folgende Komponenten konfiguriert werden:
   - Die UDP-Ports, die der RADIUS-Server für RADIUS-Authentifizierungsanforderungen und RADIUS-Autorisierungen verwendet – das sind in der Regel die Ports 1812/1813 oder 1645/1646. Diese müssen auf dem RADIUS-Server und auf allen 802.1x-fähigen Switches übereinstimmen.
   - Die IP-Adresse des Netzwerkzugriffsservers (NAS) – Ein NAS ist der Client, der RADIUS-Authentifizierungsanforderungen an den RADIUS-Server sendet. In diesem Fall sendet der Switch die Anforderung zur Benutzerauthentifizierung an den RADIUS-Server und stellt damit den NAS dar. Aus diesem Grund muss der RADIUS-Server mit der IP-Adresse jedes Switches konfiguriert werden, der im Netzwerk eine auf 802.1x basierende Authentifizierung durchführt.
   - Key String – Dies ist eine alphanumerische Zeichenfolge, die vom RADIUS-Server zur Authentifizierung des spezifischen NAS verwendet wird. Dieselbe Schlüsselzeichenfolge muss auch im entsprechenden Switch im Rahmen der Switch-Konfiguration konfiguriert werden (siehe weiter unten).
2. Vergewissern Sie sich, dass der Switch den RADIUS-Server erreicht (Ping-Signal). Der Switch kommuniziert über das Management-VLAN (in diesem Beispiel VLAN 1) mit dem RADIUS-Server und verwendet dabei seine Management-IP-Adresse als die Quell-IP-Adresse.
3. Vergewissern Sie sich, dass im RADIUS-Server mindestens ein Benutzerprofil (Benutzer-ID und Passwort) für Testzwecke enthalten ist (andere Benutzer können später hinzugefügt werden). Auf einem RADIUS-Server wie Cisco ACS sind in der Regel folgende Mindestinformationen konfiguriert:
   - Benutzer-ID
   - Benutzergruppe – Vom Administrator erstellte Gruppen wie Mitarbeiter, Netzwerkadministratoren, Manager, Buchhaltung usw.
   - Benutzerpasswort
   - Der Authentifizierungstyp (PAP/CHAP usw.) für die Benutzergruppe
   - Die Liste der für die Benutzergruppe unterstützten RADIUS-Attribute (RADIUS-Wörterbuch), wenn der RADIUS-Server mehrere Listen unterstützt

Hinweis Welche Felder tatsächlich für das Benutzerprofil erforderlich sind, kann je nach RADIUS-Server variieren. Optional kann eine Benutzergruppe in einem RADIUS-Server mit zusätzlichen Informationen konfiguriert werden, die bei der Herstellung der Benutzerverbindung verwendet werden. Für eine Benutzergruppe kann beispielsweise ein VLAN angegeben werden, das nach der Benutzerauthentifizierung als PVID des Switch-Ports verwendet wird.

Switch-Konfiguration für die Verwendung eines RADIUS-Servers

Durch diese Konfiguration wird eine auf RADIUS basierende Authentifizierung am Switch aktiviert und 802.1x für die Switch-Ports e2 bis e48 konfiguriert.

Speichern Sie bei der Switch-Konfiguration die Konfigurationsdaten regelmäßig in der Startkonfigurationsdatei, weil nicht gespeicherte Konfigurationen beim Neustart des Switches verloren gehen. Gehen Sie wie folgt vor, um die Konfiguration zu speichern:

Schritt 1 Wählen Sie **Administration > File Management > Copy/Save Configuration** aus.

Die Seite „Copy/Save Configuration“ wird geöffnet.

Schritt 2 Wählen Sie den zu kopierenden Quelldateinamen als *Running configuration* aus.

Schritt 3 Wählen Sie den Zieldateinamen als *Startup configuration* aus.

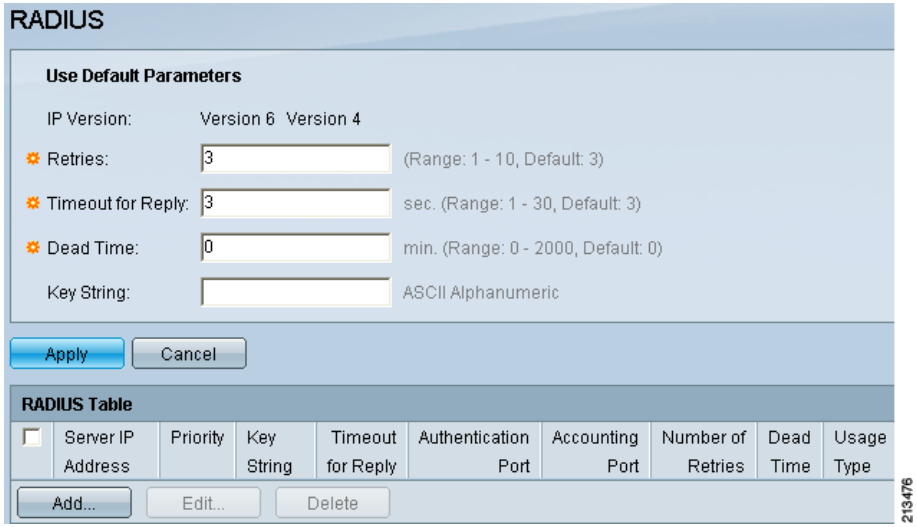
Schritt 4 Klicken Sie auf **Apply**. Dadurch wird die Konfigurationsdatei gespeichert.

Gehen Sie wie folgt vor, um den Switch für die Verwendung eines RADIUS-Servers zu konfigurieren:

Schritt 1 Wählen Sie **Security > RADIUS** aus.

Es wird der Bildschirm „RADIUS“ (Abbildung 2) angezeigt.

Abbildung 2 Bildschirm „RADIUS“

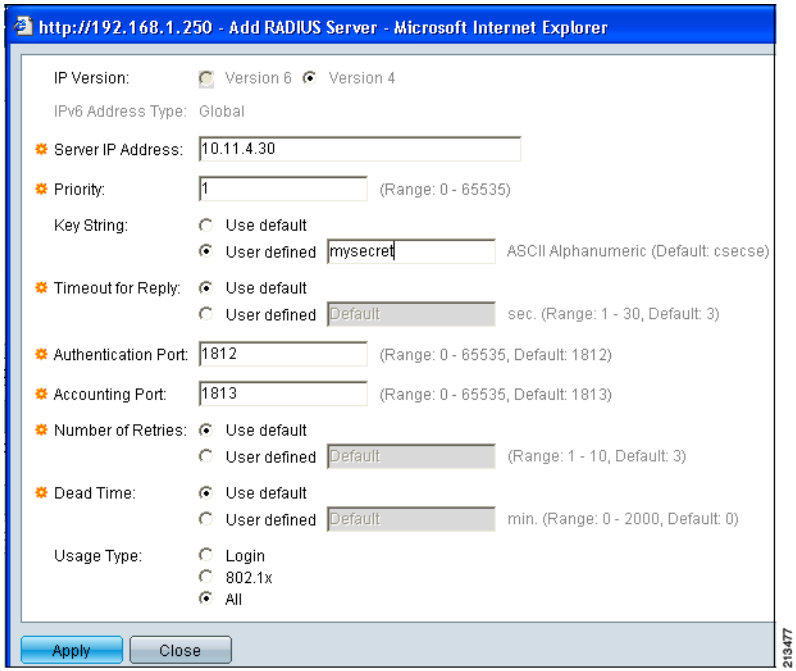


In diesem Schritt werden die Details des RADIUS-Servers (IP-Adresse und Schlüsselzeichenfolge) für den Switch angegeben, damit der Switch mit dem Server kommunizieren kann. Vergewissern Sie sich, dass keine Details des RADIUS-Servers bereits auf dem Switch konfiguriert sind. Unter der RADIUS-Tabelle dürfen also keine Details des RADIUS-Servers angezeigt werden (andernfalls wird möglicherweise der vorhandene RADIUS-Server verwendet).

Schritt 2 Um dem Switch die Informationen eines neuen RADIUS-Servers hinzuzufügen, klicken Sie auf **Add**.

Es wird der in Abbildung 3 dargestellte Popup-Bildschirm angezeigt.

Abbildung 3 Hinzufügen der Informationen eines neuen RADIUS-Servers



Schritt 3 Geben Sie die folgenden Informationen ein:

a. Server IP Address – IP-Adresse des RADIUS-Servers.

b. Priority – 1 (der erste RADIUS-Server, der kontaktiert wird).

c. Key String – Das im RADIUS-Server für diesen Switch konfigurierte gemeinsame Passwort. Der RADIUS-Server authentifiziert den Switch über dieses Passwort, und erst dann erfolgt die Benutzerauthentifizierung.

d. Authentication/Accounting Ports – Ändern Sie diese Standardeinstellungen, wenn der RADIUS-Server für die Kommunikation über andere UDP-Ports konfiguriert ist.

e. Usage Type – Wählen Sie **All** aus, damit RADIUS für die auf 802.1x basierende und für die Anmeldeauthentifizierung verwendet wird.

Schritt 4 Klicken Sie auf **Close**, um den Popup-Bildschirm zu schließen.

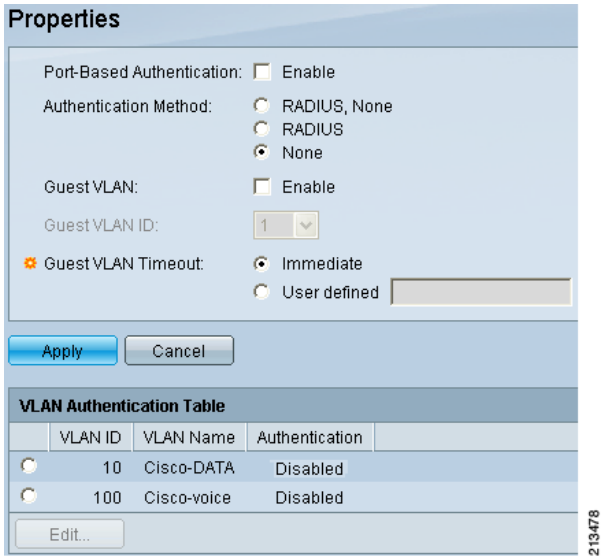
In der RADIUS-Tabelle auf dem RADIUS-Bildschirm werden jetzt die Informationen des neuen RADIUS-Servers angezeigt.

Konfiguration des Switches für den auf 802.1x basierenden authentifizierten Port-Zugriff

Schritt 1 Wählen Sie **Security > 802.1x > Properties** aus.

Es wird der Bildschirm „Properties“ (Abbildung 4) angezeigt.

Abbildung 4 Bildschirm „Properties“



Gehen Sie wie folgt vor, um 802.1x auf ausgewählten VLANs zu aktivieren und RADIUS als die Authentifizierungsrichtlinie für 802.1x anzugeben.

Schritt 2 Gehen Sie auf dem Bildschirm „Properties“ wie folgt vor:

a. Port-based Authentication – Klicken Sie auf **Enable**.

b. Authentication Method – Wählen Sie **RADIUS** aus, um eine obligatorische RADIUS-Authentifizierung festzulegen. Wenn der RADIUS-Server die Authentifizierung zurückweist oder wenn der Server nicht zur Verfügung steht, wird die Sitzung nicht zugelassen.

Die Auswahl der Option „RADIUS, None“ führt zu einem ähnlichen Ergebnis – bei einer zurückgewiesenen Authentifizierung wird die Sitzung beendet. Wenn jedoch die RADIUS-Authentifizierung nicht durchgeführt werden kann (Server/Netzwerk steht nicht zur Verfügung), wird die Sitzung zugelassen.

c. Guest VLAN – Wird in diesem Beispiel nicht verwendet.

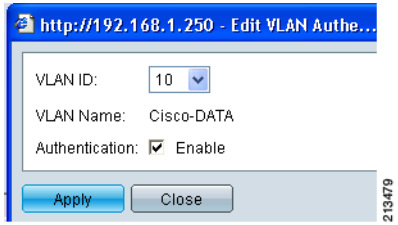
Schritt 3 Klicken Sie auf **Apply,** und vergewissern Sie sich, dass der Vorgang erfolgreich war.

Die Tabelle zur VLAN-Authentifizierung unten auf dem Bildschirm „Properties“ enthält die VLANs und zeigt an, ob die 802.1x-Authentifizierung für jedes VLAN aktiviert ist (die Authentifizierung kann standardmäßig aktiviert sein).

Schritt 4 Wählen Sie auf dem Bildschirm „Properties“ die Option **VLAN 10** aus, und klicken Sie auf **Edit**.

Es wird der in Abbildung 5 dargestellte Popup-Bildschirm angezeigt.

Abbildung 5 Bildschirm zur VLAN-Bearbeitung



Schritt 5 Gehen Sie wie folgt vor:

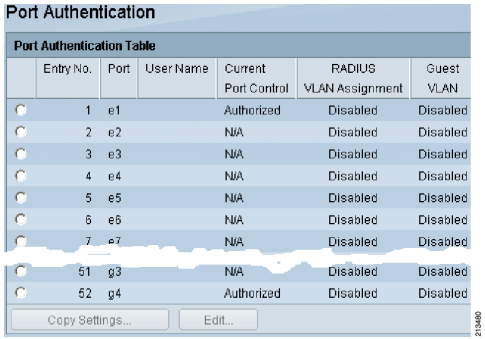
- Wenn im Feld „Authentication“ angezeigt wird, dass 802.1x auf VLAN 10 deaktiviert ist, klicken Sie auf **Enable**, um 802.1x auf VLAN 10 zu aktivieren. Klicken Sie dann auf **Apply**, und vergewissern Sie sich, dass der Vorgang erfolgreich war.
- Aktivieren Sie 802.1x entsprechend auf VLAN 100, um die 802.1x-Authentifizierung für IP-Telefone zu aktivieren. Wählen Sie dazu auf dem Bildschirm **VLAN 100** aus, und klicken Sie auf **Enable** und dann auf **Apply**.

Vergewissern Sie sich auf dem Bildschirm „Properties“, dass die 802.1x-Authentifizierung auf den jeweiligen VLANs aktiviert wurde.

Schritt 6 Wählen Sie **Security > 802.1x > Port Authentication** aus.

Es wird der in Abbildung 6 dargestellte Bildschirm „Port Authentication“ angezeigt.

Abbildung 6 Bildschirm „Port Authentication“



Auch wenn 802.1x auf den VLANs bereits aktiviert wurde, können Sie die Authentifizierung auf diesem Bildschirm für jeden Port individuell konfigurieren. Für jeden Port kann eine der folgenden Konfigurationsmöglichkeiten ausgewählt werden:

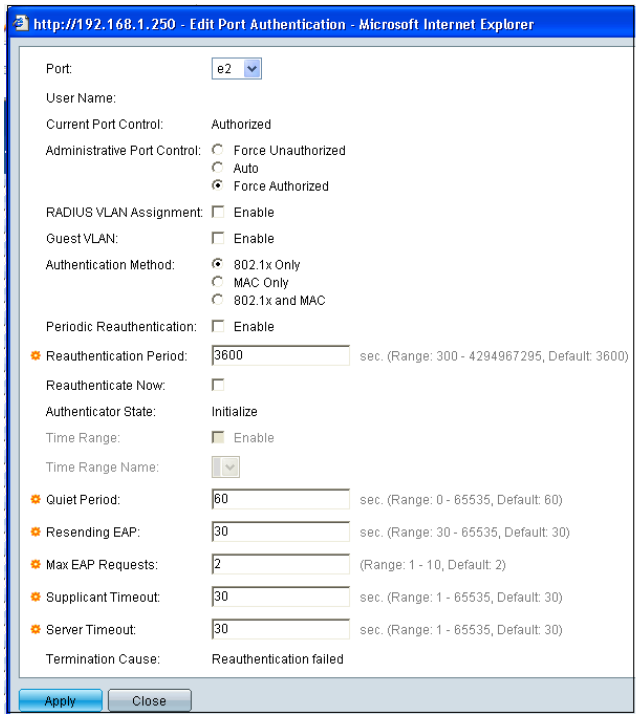
- Force Authorized – Der Port-Zugriff wird immer zugelassen (deaktivieren Sie 802.1x auf diesem Port).
- Force Unauthorized – Über den Port wird kein Zugriff zugelassen.
- Auto – Über den Port wird Zugriff nur bei erfolgreicher 802.1x-Authentifizierung zugelassen.

Damit die Auswahl der 802.1x-Authentifizierung wirksam wird, muss für den Port der Modus „Auto“ ausgewählt werden. Vor der Aktivierung dieses Modus für die betroffenen Ports ist jedoch die Konfiguration weiterer Port-Parameter erforderlich, und hierzu muss auf den Ports der Modus „Forced Authorized“ ausgewählt werden. Sie müssen also zunächst sicherstellen, dass auf den betroffenen Ports der Modus „Forced Authorized“ ausgewählt ist.

Schritt 7 Wählen Sie den Port **e2** aus, und klicken Sie auf **Edit**.

Es wird der in Abbildung 7 dargestellte Bildschirm „Edit Port Authentication“ angezeigt.

Abbildung 7 Bildschirm „Edit Port Authentication“



Schritt 8 Geben Sie, wie in Abbildung 7 dargestellt, folgende Werte in die Felder ein:

- Administrative Port Control – Wählen Sie Force Authorized aus.
- Authentication Method – Wählen Sie 802.1x Only aus.
- Falls erforderlich, können Sie zusätzlich eine regelmäßige erneute Authentifizierung auswählen. Lassen Sie die Standardwerte, wie in Abbildung 7 dargestellt, unverändert.

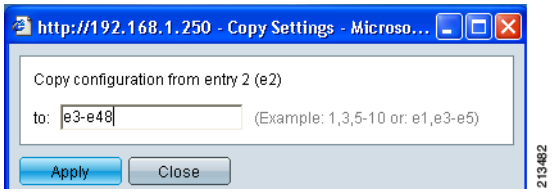
Schritt 9 Klicken Sie auf **Apply**. Vergewissern Sie sich, dass auf dem Bildschirm „Success“ angezeigt wird.

Schritt 10 Klicken Sie auf **Close**, um den Popup-Bildschirm zu schließen und den zu Grunde liegenden Bildschirm „Port Authentication“ anzuzeigen.

Schritt 11 Wählen Sie auf dem Bildschirm „Port Authentication“ den Port **e2** aus, und klicken Sie auf **Copy Settings**.

Es wird das in Abbildung 8 dargestellte Popup-Fenster „Copy Settings“ angezeigt.

Abbildung 8 Popup-Fenster „Copy Settings“



Schritt 12 Geben Sie den Port-Bereich (z. B. **e3–e48**) ein, um die Konfiguration von e2 zu kopieren.

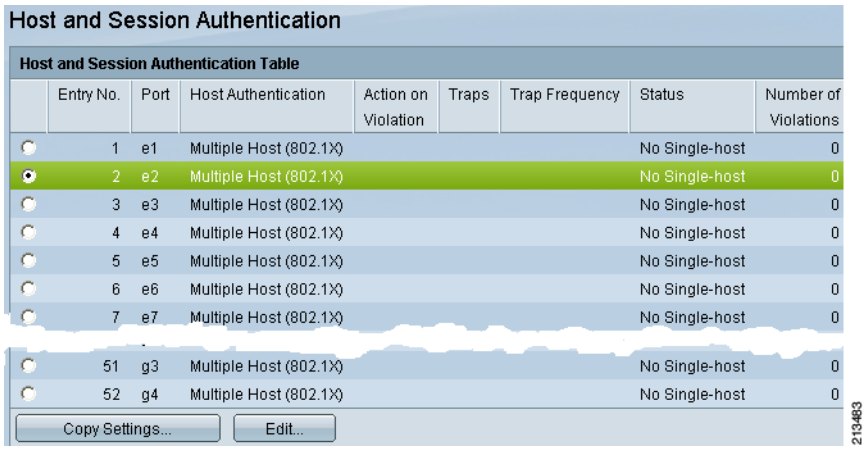
Schritt 13 Klicken Sie auf **Apply,** und vergewissern Sie sich, dass auf dem Bildschirm „Port Authentication“ die Meldung „Success“ angezeigt wird.

Die Ports können jetzt im Modus „Forced Authorized“ in den Port-Bereich kopiert werden.

Schritt 14 Wählen Sie **Security > 802.1x > Hosts and Session Authentication** aus.

Es wird der Bildschirm „Host and Session Authentication“ (Abbildung 9) angezeigt, auf dem Sie Zugriffsrichtlinien angeben können, die bei der Verbindung mehrerer Gerät mit dem Port verwendet werden.

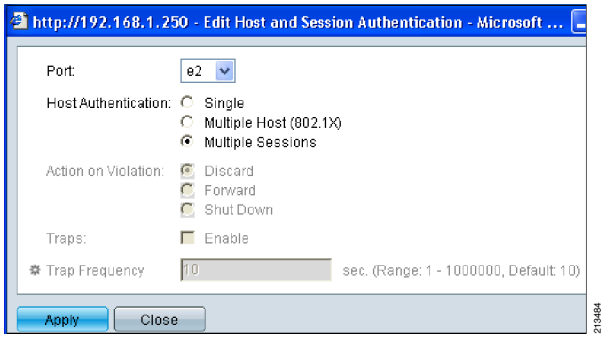
Abbildung 9 Bildschirm „Host and Session Authentication“



Schritt 15 Um die Richtlinie für Port **e2** zu ändern, wählen Sie den Port **e2,** wie in Abbildung 9 dargestellt, aus, und klicken Sie auf **Edit**.

Es wird, wie in Abbildung 10 dargestellt, der Popup-Bildschirm „Edit Hosts and Session Authentication“ angezeigt.

Abbildung 10 Popup-Bildschirm „Edit Hosts and Session Authentication“



Schritt 16 Wählen Sie im Feld „Host Authentication“ die Option **Multiple Sessions** aus, und klicken Sie auf **Apply**.

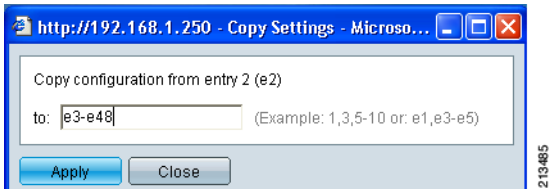
Vergewissern Sie sich, dass „Success“ angezeigt wird.

Wenn der Vorgang zurückgewiesen wird, kehren Sie zum 7. Schritt zurück, ändern Sie den Wert im Feld „Administrative Port Control“ zu **Force Authorized,** und versuchen Sie es erneut.

Schritt 17 Wählen Sie auf dem Bildschirm „Host and Session Authentication“ den Port **e2** aus, und klicken Sie auf **Copy Settings**.

Es wird das in Abbildung 11 dargestellte Popup-Fenster „Copy Settings“ angezeigt.

Abbildung 11 Popup-Fenster „Copy Settings“



Schritt 18 Geben Sie den Port-Bereich (z. B. **e3–e48**) ein, um die Konfiguration von e2 auf die angegebenen Ports zu kopieren, und klicken Sie auf **Apply**.

Vergewissern Sie sich, dass auf dem Bildschirm „Host and Session Authentication“ die Meldung „Success“ angezeigt wird.

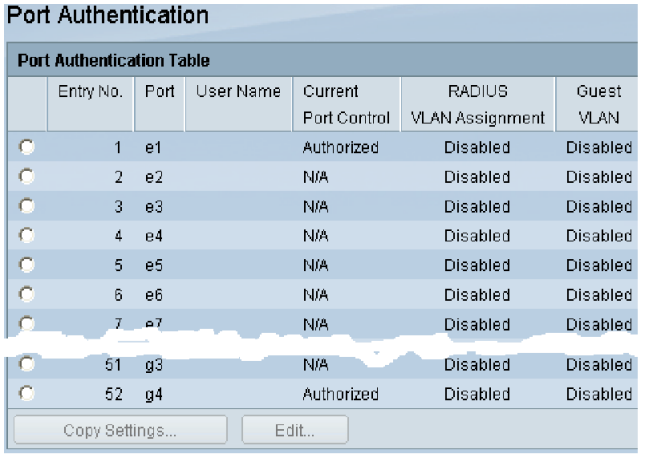
Die Ports können jetzt im Modus „Multiple Session“ der Host-Authentifizierung in den Port-Bereich kopiert werden.

In nächsten Schritt wird die 802.1x-Authentifizierung zu Überprüfungszwecken für einen einzelnen Port (e2) aktiviert. Nachdem die korrekte Funktionsweise überprüft wurde, kann 802.1x auf anderen Ports aktiviert werden.

Schritt 19 Um die 802.1x-Authentifizierung auf dem Port e2 zu aktivieren, wählen Sie **Security > 802.1x > Port Authentication** aus.

Der Bildschirm „Port Authentication“ wird, wie in Abbildung 12 dargestellt, angezeigt.

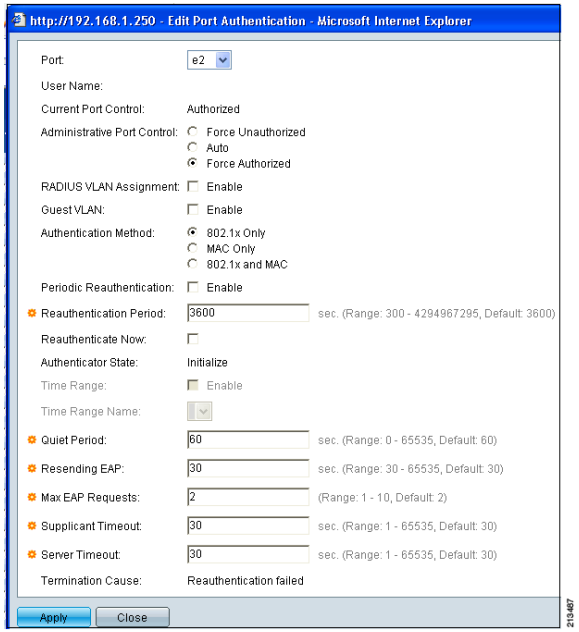
Abbildung 12 Bildschirm „Port Authentication“



Schritt 20 Wählen Sie den Port **e2** aus, und klicken Sie auf **Edit**.

Es wird der in Abbildung 13 dargestellte Bildschirm „Edit Port Authentication“ angezeigt.

Abbildung 13 Bildschirm „Edit Port Authentication“



Schritt 21 Geben Sie in die Felder folgende Werte ein:

- Administrative Port Control – Wählen Sie **Auto** aus.
- Authentication Method – Wählen Sie **802.1x Only** aus.
- Falls erforderlich, können Sie zusätzlich eine regelmäßige erneute Authentifizierung auswählen. Lassen Sie die Timeout-Standardwerte, wie in Abbildung 13 dargestellt, unverändert.

Schritt 22 Klicken Sie auf **Apply**, und vergewissern Sie sich, dass auf dem Bildschirm „Success“ angezeigt wird.

Schritt 23 Klicken Sie auf **Close**, um den Popup-Bildschirm zu schließen und den zu Grunde liegenden Bildschirm „Port Authentication“ anzuzeigen.

Damit ist die 802.1x-Konfiguration auf dem Port e2 abgeschlossen.

Schritt 24 Um sicherzustellen, dass 802.1x auf dem Port e2 funktioniert, schließen Sie einen Laptop an den Port e2 an, und konfigurieren Sie die Ethernet-Verbindung des Laptops für Folgendes:

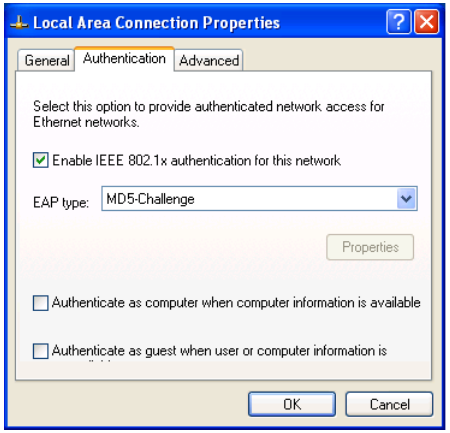
- Annahme von IP-Adresse und DNS über DHCP
- Durchführung einer 802.1x-Authentifizierung

Welche Bildschirme angezeigt werden, kann je nach Typ und Version des Betriebssystems auf dem Laptop variieren. Das angegebene Beispiel zeigt die Bildschirme bei Windows XP.

Schritt 25 Wählen Sie **Local Area Connection Properties > General > Authentication** aus.

Es wird der in Abbildung 14 dargestellte Bildschirm angezeigt.

Abbildung 14 Eigenschaften von LAN-Verbindung – Registerkarte „Authentifizierung“



Schritt 26 Aktivieren Sie das Kontrollkästchen **IEEE 802.1x Authentication**.

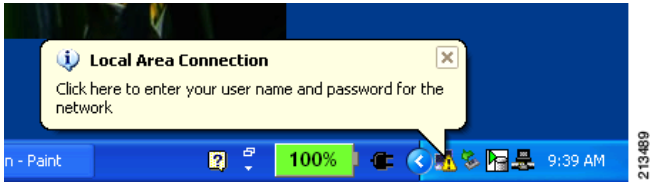
Schritt 27 Wählen Sie als EAP-Typ je nachdem **MD5-Challenge** oder **PEAP** aus.

Diese Auswahl muss mit dem im RADIUS-Server konfigurierten Authentifizierungstyp für die Benutzergruppe übereinstimmen.

Schritt 28 Klicken Sie auf **OK**, um die geänderte Konfiguration zu speichern.

Nach dem Anschluss des Laptops wird auf dem Laptop möglicherweise einige Sekunden lang angezeigt, dass eine Verbindung besteht, obwohl dem Benutzer kein Zugriff erteilt wird. Nach einigen weiteren Sekunden sollte, wie in Abbildung 15 dargestellt, eine Meldung angezeigt werden, in der Sie zur Eingabe von Benutzername und Passwort aufgefordert werden.

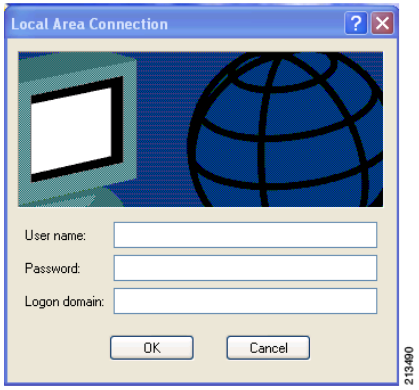
Abbildung 15 Eingabe von Benutzername und Passwort



Schritt 29 Klicken Sie auf das angezeigte Symbol.

Es wird der in Abbildung 16 dargestellte Bildschirm angezeigt, auf dem Sie zur Authentifizierung den Benutzernamen und das Passwort eingeben können.

Abbildung 16 Bildschirm für die Benutzerauthentifizierung



Schritt 30 Geben Sie den Benutzernamen und das Passwort ein, und klicken Sie auf **OK**.

Die auf 802.1x-basierende Authentifizierung wird nun abgeschlossen, und das Verbindungssymbol des Laptops auf der Taskleiste zeigt an, dass eine Verbindung hergestellt wurde.

Schritt 31 Wählen Sie **Security > 802.1x > Port Authentication** aus.

Es wird der Bildschirm „Port Authentication“ (Abbildung 12) mit einer Tabelle angezeigt, in der der authentifizierte Status der Ports angegeben ist. Vergewissern Sie sich, dass der Port e2 jetzt unter der Spalte „Current Port Control“ mit dem Status „Authorized“ aufgeführt ist.

Schritt 32 Wählen Sie **Security > 802.1x > Authenticated Hosts** aus.

Es wird der Bildschirm „Authenticated Hosts“ mit allen Ports angezeigt, die aktuell nach 802.1x authentifiziert sind. Für jeden authentifizierten Port wird die entsprechende Benutzer-ID, die MAC-Adresse des Benutzergeräts (z. B. ein Laptop) und die Sitzungszeit angezeigt. Vergewissern Sie sich, dass die hier für den Port e2 angezeigten Informationen richtig sind.

Sie können jetzt ein Ping-Signal an die IP-Adressen im Netzwerk senden, um sicherzustellen, dass der Port den Benutzerverkehr zulässt.

Damit ist die 802.1x-Verifizierung für den Port e2 abgeschlossen.

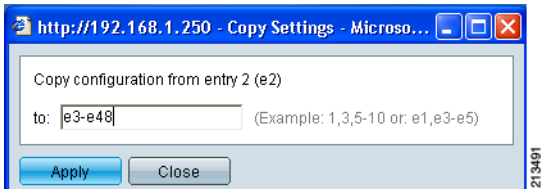
Schritt 33 Um die 802.1x-Authentifizierung für andere Ports (in diesem Beispiel e2–e48) zu aktivieren, wählen Sie **Security > 802.1x > Port Authentication** aus.

Es wird der Bildschirm „Port Authentication“ angezeigt.

Schritt 34 Wählen Sie den Port **e2** aus, und klicken Sie auf **Copy Settings**.

Es wird das in Abbildung 17 dargestellte Popup-Fenster „Copy Settings“ angezeigt.

Abbildung 17 Popup-Fenster „Copy Settings“



Schritt 35 Geben Sie den Port-Bereich (z. B. **e3–e48**) ein, um die Konfiguration von e2 auf die angegebenen Ports zu kopieren, und klicken Sie auf **Apply**.

Vergewissern Sie sich, dass auf dem Bildschirm „Port Authentication“ die Meldung „Success“ angezeigt wird.

Dadurch wird 802.1x für den angegebenen Port-Bereich aktiviert.

Konfiguration eines zeitabhängigen Port-Zugriffs (optional)

Durch diese Konfiguration wird ein Port für einen absoluten Zeitraum vom 17. August 2010 bis zum 1. Januar 2020 eingerichtet. Der Benutzerzugriff wird außerdem auf bestimmte Zeiten eines Wochentags beschränkt (z. B. Montag von 9 bis 17 Uhr).

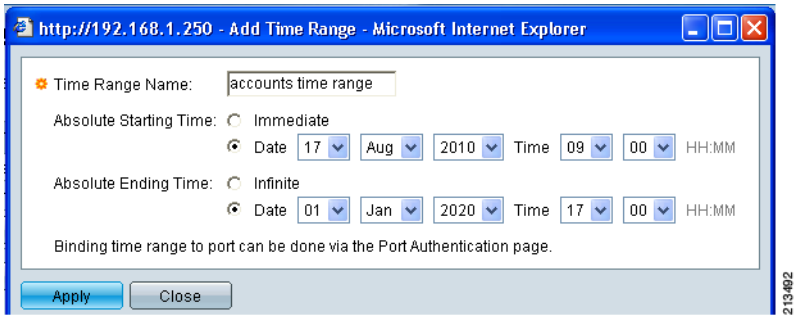
Schritt 1 Wählen Sie **Security > 802.1x > Time Range** aus.

Es wird der Bildschirm „Time Range“ angezeigt, auf dem Sie einen absoluten Zeitraum hinzufügen können.

Schritt 2 Klicken Sie auf **Hinzufügen**.

Es wird der in Abbildung 18 dargestellte Popup-Bildschirm angezeigt.

Abbildung 18 Hinzufügen eines Zeitraums



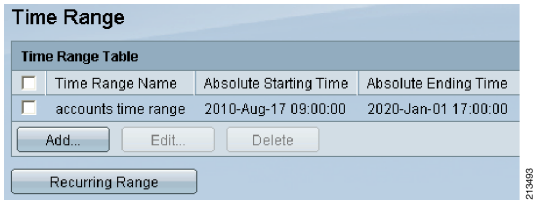
Schritt 3 Geben Sie, wie in Abbildung 18 dargestellt, einen Namen für den absoluten Zeitraum (**accounts time range**) und dessen Startzeit, Startdatum, Endzeit und Enddatum ein.

Alternativ können Sie für die Startzeit auch „Immediate“ und/oder für die Endzeit „Infinite“ auswählen.

Schritt 4 Klicken Sie auf **Apply**, und vergewissern Sie sich, dass „Success“ angezeigt wird.

Es wird der in Abbildung 19 dargestellte Bildschirm mit dem neu eingegebenen Zeitraum angezeigt.

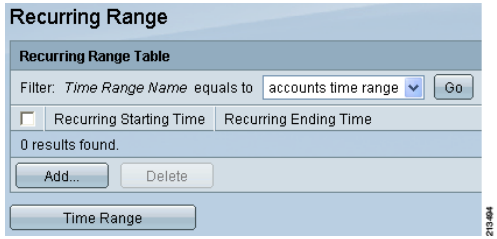
Abbildung 19 Bildschirm „Time Range“



Schritt 5 Klicken Sie auf **Recurring Range**.

Es wird, wie in Abbildung 20 dargestellt, der Bildschirm „Recurring Range“ angezeigt.

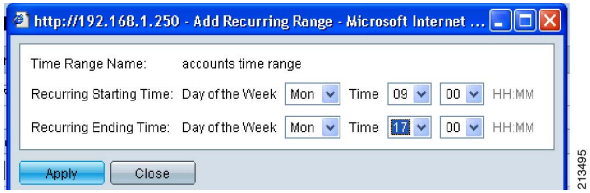
Abbildung 20 Bildschirm „Recurring Range“



Schritt 6 Klicken Sie auf **Add...**

Es wird, wie in Abbildung 21 dargestellt, der Bildschirm „Add Recurring Range“ angezeigt, über den dem ausgewählten absoluten Zeitraum (in diesem Beispiel „accounts time range“) ein oder mehrere sich wiederholende Zeiträume hinzugefügt werden können.

Abbildung 21 Abbildung 23



Schritt 7 Geben Sie, wie in Abbildung 21 dargestellt, für jeden Wochentag einen Wert bei „Recurring Starting Time“ und bei „Recurring Ending Time“ ein, und klicken Sie auf **Apply**.

Vergewissern Sie sich, dass „Success“ angezeigt wird.

Wie in Abbildung 21 dargestellt, wird dadurch ein sich wiederholender Zeitraum für Montag von 9 bis 17 Uhr eingerichtet. Der Zugriff ist nur in diesem Zeitraum und nur bei erfolgreicher 802.1x-Authentifizierung zulässig.

Wiederholen Sie die Schritte 5 und 6, um für die anderen Wochentage weitere sich wiederholende Zeiträume hinzuzufügen.

Damit ist die Einrichtung bestimmter Zeiträume abgeschlossen. Sie müssen diese Einstellung nun auf die Ports anwenden.

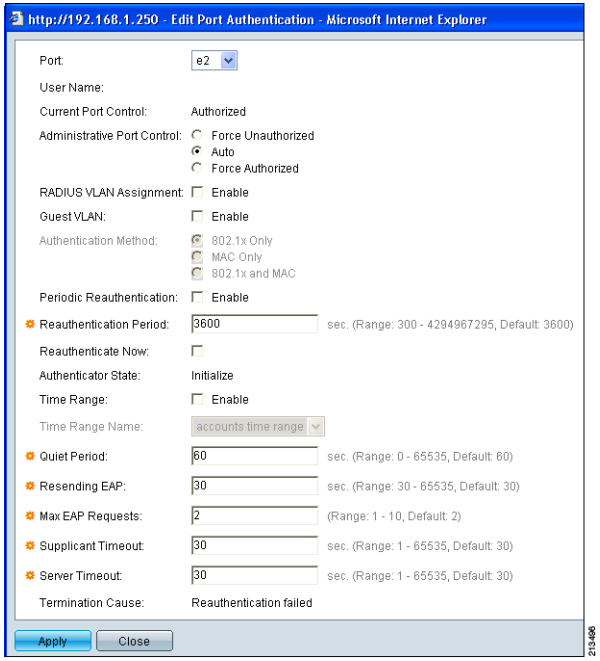
Schritt 8 Wählen Sie **Security > 802.1x > Port Authentication** aus.

Es wird der Bildschirm „Port Authentication“ mit allen Ports und deren Informationen angezeigt.

Schritt 9 Wählen Sie einen Port aus (in diesem Beispiel **e2**), für den der Zeitbereich angewendet werden soll, und klicken Sie auf **Edit**.

Der in Abbildung 22 dargestellte Bildschirm wird mit Informationen des Ports angezeigt. Das Feld „Time Range“ ist auf diesem Bildschirm nicht standardmäßig aktiviert.

Abbildung 22 Bildschirm „Edit Port Authentication“



Schritt 10 Gehen Sie wie folgt vor, um dem Port e2 den Zeitraum hinzuzufügen:

a. Klicken Sie, um das Feld „Time Range“ zu aktivieren.

b. Wählen Sie im Feld „Time Range“ aus der Dropdown-Liste einen Zeitraum aus (in diesem Fall „accounts time range“).

Schritt 11 Klicken Sie auf **Apply**.

Vergewissern Sie sich, dass auf dem Bildschirm „Edit Port Authentication“ die Meldung „Success“ angezeigt wird.

Schritt 12 Klicken Sie auf **Close**, um den Bildschirm „Edit Port Authentication“ zu schließen.

Der Zeitraum ist jetzt für den Port e2 konfiguriert.

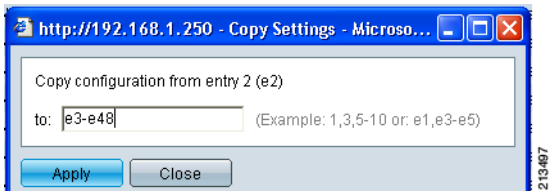
Schritt 13 Wählen Sie **Security > 802.1x > Port Authentication** aus.

Es wird der Bildschirm „Port Authentication“ mit allen Ports und deren Informationen angezeigt. Die Konfiguration des Ports e2 kann damit auf ähnliche Ports kopiert werden.

Schritt 14 Wählen Sie einen Port aus (in diesem Beispiel e2), auf den der Zeitraum angewendet wurde, und klicken Sie auf **Copy Settings**.

Auf dem in Abbildung 23 dargestellten Bildschirm können die Ports eingegeben werden, auf die die Konfiguration des Ports e2 kopiert werden soll.

Abbildung 23 Bildschirm für das Kopieren der Konfiguration



Schritt 15 Geben Sie den Bereich ein (z. B. e2–e48), und klicken Sie auf **Apply**.

Dieser Bildschirm wird geschlossen, und der Bildschirm „Port Authentication“ wird aktualisiert.

Schritt 16 Vergewissern Sie sich, dass auf dem Bildschirm„Port Authentication“ die Meldung „Success“ angezeigt wird.

Damit ist die 802.1x-Konfiguration für die Ports e2 bis e48 abgeschlossen.

Zusammenfassung

In diesem Dokument wird die Verwendung der 802.1x-Authentifizierung und deren Konfiguration auf einem Cisco Small Business-Switch der Serie 300 beschrieben. Dies ermöglicht die Einrichtung eines authentifizierten Zugriffs auf die LAN-Ports, um die Netzwerksicherheit zu erhöhen. Die Unterstützung eines zeitbasierten Zugriffs, bei dem der Port-Zugriff weiter auf spezifische Ports und bestimmte Tageszeiten eingeschränkt wird, sorgt für noch mehr Sicherheit. Daneben kann das VLAN über die dynamische VLAN-Zuordnung (DVA) automatisch einem Benutzer zugeordnet werden, sodass Ports nicht mit VLANs vorkonfiguriert werden müssen. Durch diese Verfahren können LANs sicherer und flexibler bereitgestellt werden.

Weitere Informationen zur Konfiguration der Cisco Managed Switches der Serie 300 finden Sie im Administratorhandbuch unter der folgenden URL:

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