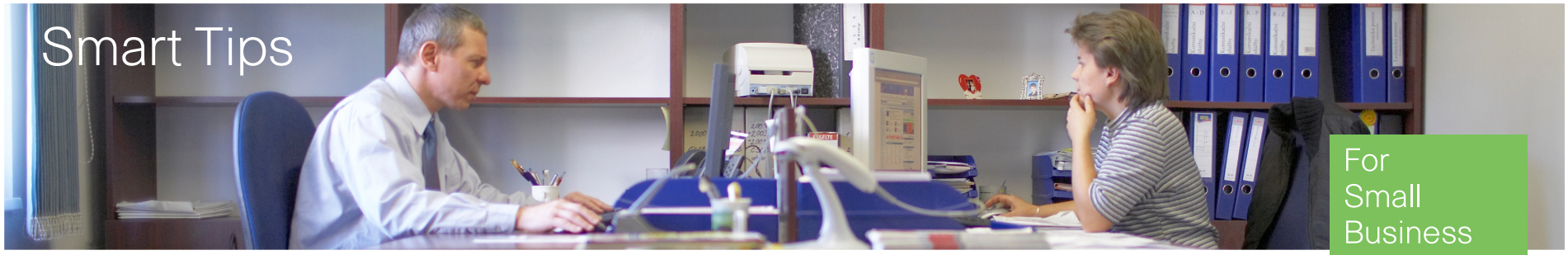


Authenticated and Time-Based Network Access with 802.1x

802.1x is an IEEE standard for controlling access to a network on a per-port basis. Cisco Small Business 300 Series switches support 802.1x to provide better network security. In an 802.1x-enabled network, a user device such as a laptop or an IP phone requests port access to its directly connected switch. The switch gets the user ID and password of the user (or device) and forwards them to a RADIUS server for authentication. The switch allows access to the port only if the user authentication is successful. Such authenticated access to a LAN improves network security.

Featured Products

This Smart Tip describes using 802.1x based authentication on a Cisco Small Business 300 Series Managed Switch (model SF300-48P) with various Power over Ethernet (PoE) and non-PoE switch ports. For details about other Cisco 300 Series Managed Switches, visit: http://www.cisco.com/go/300switches.

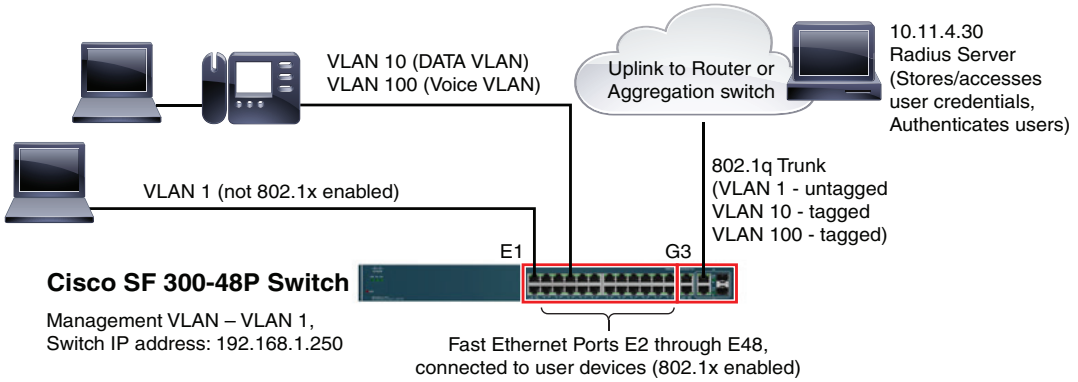
802.1x-Enabled Network Design

The main components of a network with 802.1x-based authentication, as shown in Figure 1, are as follows:

- Laptop/IP phones (or other similar end-user devices that can request 802.1x-based access to a network)
- A switch that authenticates the user using a RADIUS server, and allows network access only when authentication is successful
- A RADIUS server to authenticate the user

When 802.1x authentication is enabled in a LAN, it is typical to enable it on all switch ports that are intended to be connected to end-user devices or other devices requiring such authenticated port access.

Figure 1 Authenticated Network Access using 802.1x



Authentication

To authenticate a user, the RADIUS server accesses a user database that contains information such as user ID, password, and other optional information that it provides the switch on successful authentication. The database can be integrated into the RADIUS server, or be an external one such as an Active Directory.

Which Ports to Authenticate?

802.1x-based authentication is primarily intended for end-user devices such as laptops or IP phones that are untrusted devices from a security standpoint. Therefore, 802.1x is not configured on ports connected to network devices such as routers, switches, or servers, or any such trusted devices. It is configured on ports intended for connecting user devices on an access switch, and also on an aggregation switch if user devices can be directly connected to it.

Port Authentication Policy

The Cisco Small Business 300 Series switch port can be configured with one of the following three policies that determine how 802.1x-based authentication affects port access when multiple devices can potentially be attached to a single port:

- Single—Allows only a single authorized host to access the port.
- Multiple host (802.1x)—The port supports multiple hosts. Only the first host must be 802.1x authorized. If the authorization is successful, not only the authenticated device but all other attached devices can access the port with no additional authentication. Until authentication of at least one attached device is successful, no device can access the port. This is useful for deploying devices that do not support 802.1x.
- Multiple sessions—Allows multiple hosts to access the port, but each must be individually and separately authenticated.

Note The multiple sessions policy is recommended in Cisco SMART Designs for better flexibility and security. The multiple host policy can be used to support devices on a port that does not support 802.1 x authentication.

Note The Cisco Small Business 300 Series switch can be configured to put a user into the Guest VLAN when the user fails 802.1x authentication.

RADIUS Server Considerations

The Cisco Small Business 300 Series switch accesses the RADIUS server over the management VLAN, using the single management IP address assigned to the switch (being a Layer 3-capable switch, the switch can support multiple IP interfaces as well). This implies that the switch should be able to use its management VLAN to reach the RADIUS server. If the RADIUS server is on a different VLAN (as assumed in Figure 1), the WAN router typically performs the necessary inter-VLAN routing.

The WAN router terminates the management VLAN. If the factory-default management VLAN (VLAN 1) is used, the LAN switches must be configured to forward the untagged VLAN 1 along with other VLANs, if any, through their trunk ports to the WAN router.

Authenticating IP Phones

IP phones can be 802.1x authenticated as well as PCs and laptops. Cisco IP phones are 802.1x enabled. For details on enabling 802.1x authentication on the IP phone and to create an appropriate user ID for the IP phone in the RADIUS server, see the administrator guide for the specific IP phone.

Time-based Authentication

The Cisco Small Business 300 Series switch allows you to restrict access to the 802.1x-enabled ports to a specified time range, which specifies an absolute time range such as 9 AM, Feb 22nd, 2010 to 5 PM, April 30th, 2023. In this case, users are allowed authenticated port access at any time during the specified period. Outside the time period, the ports are in a “Force Unauthorized” state, which means they cannot be accessed, and no 802.1x authentication is initiated.

After you set up an absolute time range, you can optionally refine it by adding a recurring time range to it. A recurring time range further restricts user access to a start and an end time specific to each day in a week (you can define separate time periods for different days of a week).

Ports can be assigned different time ranges. This is helpful if the work hours (or network access hours) of employees vary.

Dynamic VLAN Assignment

Dynamic VLAN Assignment (DVA) dynamically assigns a user-specific VLAN to a port after successful 802.1x authentication. The VLAN corresponding to the user must be defined in the user RADIUS profile. When the user is successfully authenticated, the RADIUS server provides the user’s VLAN information to the switch as part of the authentication procedure. The switch then adds the port as an untagged member of that VLAN. This helps user mobility when different users belong to separate data VLANs based on their departments, or some other criteria.

Although the Cisco Small Business 300 Series switch supports DVA, this document does not cover configuration of this feature. For more information, see the administration guide at the following URL: http://www.cisco.com/en/US/docs/switches/lan/csbms/sf30x_sg30x/administration_guide/78-19308-01.pdf.

Configuration Tips

This section provides a configuration example of 802.1x for a Cisco Small Business 300 Series switch. Specifically, the example configures the Fast Ethernet ports from e2 through e48 of a Cisco SF 300-48P switch to enable authenticated port access using 802.1x.

This section refers to the configuration of an access switch in a Cisco SMART Design topology as shown in Figure 1.

Network Prerequisites for this Configuration

LAN Prerequisites

1. All switch ports of a Cisco Small Business 300 Series switch are associated with the native VLAN 1 as factory default. In practice, it is often necessary to create other separate VLANs for data and voice. This configuration example uses VLAN 10 as the data VLAN and VLAN 100 as the voice VLAN.

   As an example, a single port (e1) is assigned to VLAN 1 and is intended to be used as a dedicated management port. However, note that in practice, VLAN 10 (data VLAN) may be used as the management VLAN as well. Also, using dedicated management ports is optional.
2. All these VLANs (VLANs 10, 100, and 1) are terminated at the WAN router.
3. The Cisco 300 Series switch can configure a port in the following three ways:
   - Access port—The port can be associated with a single VLAN, which is called the Port VLAN ID (PVID). An access port places all incoming packets through the port in the PVID. It can support only a single VLAN, and thus is not suitable if separate voice and data VLANs are used.
   - Trunk port—The port can support a single PVID and one or more 802.1q encapsulated (tagged) VLANs. As shown in Table 1, this design uses trunk ports.
   - General port—This can support multiple untagged and tagged VLANs, where untagged traffic is placed into VLANs based on the source MAC addresses.

This configuration assumes that the access switch is configured as shown in Table 1. The actual VLAN numbers and ports used can change in a deployment depending on specific requirements (see Figure 1).

Table 1 Port Configurations for this Example

	Port #	Port Type	Port VLAN (PVID)	Tagged VLANs	Excluded VLANs
Specific switch management interface, (optional)	e1	Trunk	VLAN 1		10, 100
Ports connected to users laptops/IP phones	e2 through e48	Trunk	VLAN 10 (data VLAN)	VLAN 100 (voice VLAN)	1
Upstream port	G3 (also G1, G2, G4)	Trunk	VLAN 1	VLANs 10, 100	1

4. The switch has Rapid Spanning Tree Protocol enabled, and it can forward traffic through the LAN using its VLANs.

Aggregation Switch Configuration

This configuration assumes that the aggregation switch is configured as described in Table 2.

Table 2 Aggregation Switch Configuration

	Port Attached to the Cisco 300 Series switch	Port Attached to the WAN Router
VLAN 1	Untagged (PVID)	Untagged (PVID)
VLAN 10	Tagged	Tagged
VALN 100	Tagged	Tagged

Note Specifically, verify that the aggregation switch is configured to forward the untagged VLAN 1 (for example, if a Cisco Catalyst switch is used, the untagged VLAN must be included in the VLANs to be allowed through the trunk port via a command such as switchport trunk allowed vlan 1,10,100).

WAN Router Configuration Prerequisites

It is assumed that the WAN router terminates the VLANs as shown in Table 3.

Table 3 WAN Router VLAN Termination

	Router's Port Attached to the Cisco 300 Series Switch	
	VLAN Interface Type	IP Address (Default Gateway for the Subnet)
VLAN 1	Native VLAN (untagged)	192.168.1.1
VLAN 10	Tagged	10.1.20.1
VLAN 100	Tagged	10.1.100.1

RADIUS Server Configuration Prerequisites

1. Verify that the RADIUS server is configured to accept RADIUS authentication requests for the specific switch; that is, the switch IP address and the key string (shared password) are specified in the RADIUS server. This means configuring the following on the RADIUS server:
   - The UDP ports used by the RADIUS server to listen to RADIUS Authentication requests and RADIUS Authorizations—typically, these are either 1812/1813 or 1645/1646. They must match between the RADIUS server and all the 802.1x-enabled switches.
   - Network Access Server (NAS) IP address—A NAS is the client that sends RADIUS authentication requests to the RADIUS server. In this case, the switch sends the user authentication requests to the RADIUS server, and thus is the NAS. Therefore, the RADIUS server must be configured with the IP address of each switch that performs 802.1x-based authentication in the network.
   - Key string—This is an alphanumeric string that is used by the RADIUS server to authenticate the specific NAS. The same key string must also be configured in the corresponding switch as part of the switch configuration (see below).
2. Verify that the switch can reach (ping) the RADIUS server. The switch talks with the RADIUS server over the management VLAN (VLAN 1, in this example) using its management IP address as the source IP address.
3. Verify that the RADIUS server is populated with at least one user profile (user ID and password) for testing (other users can be added later). Usually, the minimum information configured for a user on a RADIUS server such as Cisco ACS is as follows:
   - User ID
   - User group—Administrator-created groups such as regular employee, network administrators, managers, accounts department, and so on
   - User password
   - The type of authentication (PAP/CHAP, and so on,) associated with the user group
   - The list of RADIUS attributes (RADIUS dictionary) supported for the user group, if more than one list are supported by the RADIUS server

Note The exact fields necessary for the user profile may vary depending on the RADIUS server. Optionally, a user group in a RADIUS server may be configured with additional information used while establishing the user connection. For example, the user group may specify a VLAN to use as the PVID of the switch port, after the user is authenticated.

Configuring the Switch for using a RADIUS Server

This configuration enables RADIUS-based authentication on the switch, and configures 802.1x on the switch ports e2 through e48.

While configuring the switch, save the configuration frequently to the startup configuration file, because unsaved configurations are lost when the switch is rebooted. The following steps save the configuration:

Step 1 Select **Administration > File Management > Copy/Save Configuration**.

The Copy/Save Configuration page opens.

Step 2 Select the Source File Name to be copied as *Running configuration*.

Step 3 Select the Destination File Name as *Startup configuration*.

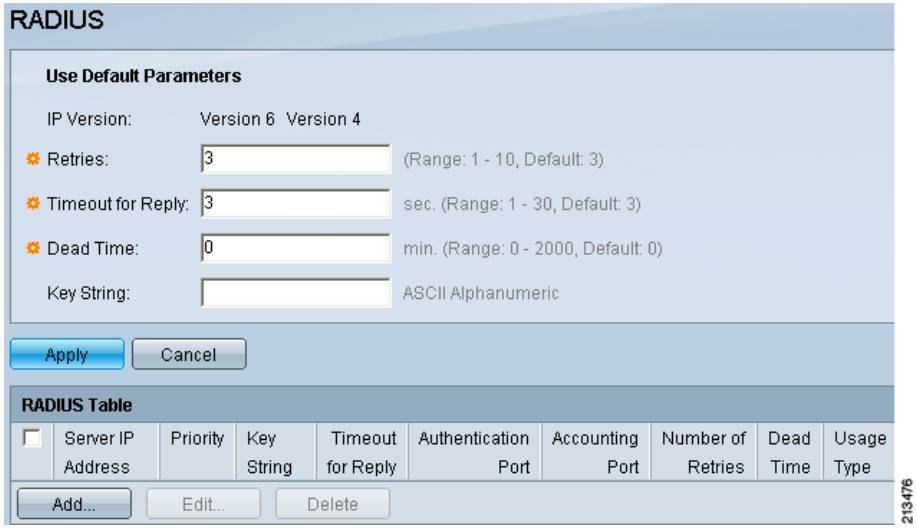
Step 4 Click **Apply**. This saves the configuration file.

To configure the switch for using a RADIUS server, complete the following steps.

Step 1 **Step 1** Select **Security > RADIUS**.

The RADIUS screen (Figure 2) is displayed.

Figure 2 RADIUS Screen

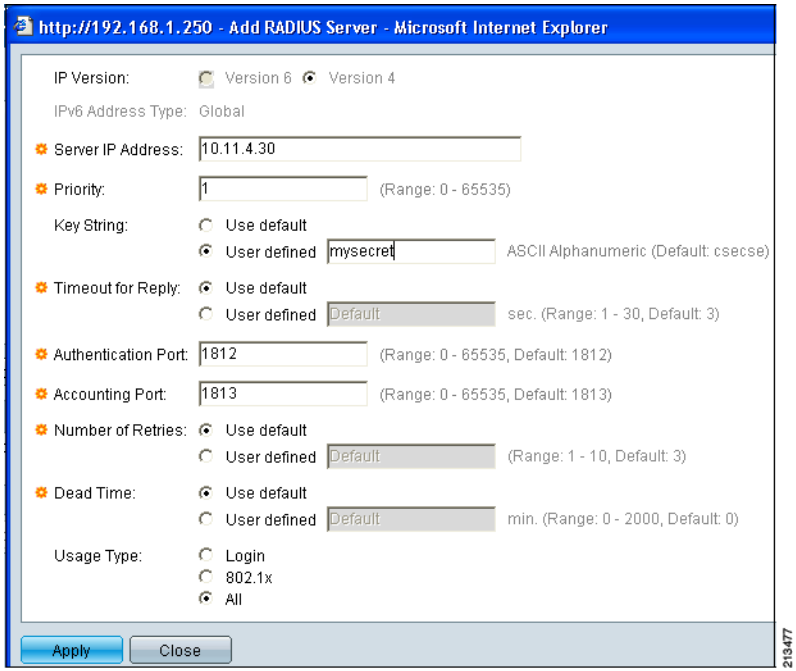


This step specifies the details of the RADIUS server (IP address and key string) to the switch, so that the switch can communicate with it. Check that no RADIUS server details are already configured on the switch; that is, no RADIUS server details appear below the RADIUS table (otherwise, you may use the existing RADIUS server).

Step 2 To add a new RADIUS server's information to the switch, click **Add**.

The popup screen in Figure 3 is displayed.

Figure 3 Adding New RADIUS Server Information



Step 3 Enter the following information:

a. Server IP address—IP address of RADIUS server.

b. Priority—1 (the first RADIUS server to contact).

c. Key string—The shared password configured in the RADIUS server for this switch. RADIUS server authenticates the switch using this password before performing any user authentication.

d. Authentication and access ports—Change these defaults if the RADIUS server is configured to communicate using some other UDP ports.

e. Usage type—Select **All**, signifying that RADIUS will be used to do both 802.1x-based and login authentication.

Step 4 Click **Close** to remove the popup screen.

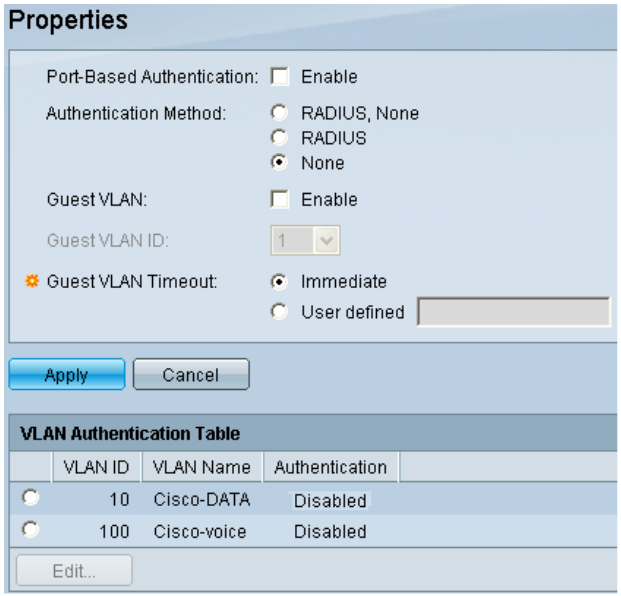
The RADIUS table in the RADIUS screen now displays the new RADIUS server information.

Configuring the Switch for 802.1x-based Authenticated Port Access

Step 1 Select **Security > 802.1x >Properties**.

The Properties screen (Figure 4) is displayed.

Figure 4 Properties Screen



The following steps enable 802.1x on selected VLANs, and specify RADIUS as the authentication policy for 802.1x.

Step 2 In the Properties screen, do the following:

a. Port-based Authentication—Click **Enable**.

b. Authentication Method—Select **RADIUS**, to indicate mandatory RADIUS authentication. If the RADIUS server rejects the authentication, or if the server is down, the session is not permitted.

Choosing the "RADIUS, None" option is similar in that an authentication rejection terminates the session. However, if the RADIUS authentication cannot be completed (server/network down), the session is permitted.

c. Guest VLAN—Not used in this example.

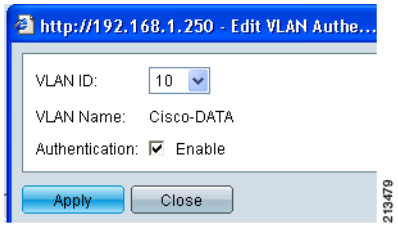
Step 3 Click **Apply**, and verify success of the operation.

The VLAN Authentication table at the bottom of the Properties screen shows the VLANs and whether 802.1x authentication is enabled on each VLAN (by default, it may be enabled).

Step 4 In the Properties screen, select **VLAN 10** and click **Edit**.

This displays the popup screen shown in Figure 5.

Figure 5 Edit VLAN Screen



Step 5 Do the following:

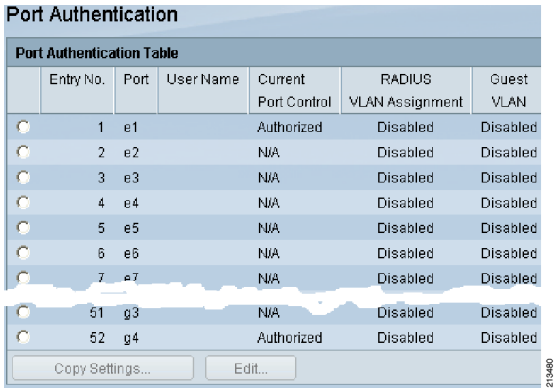
- If the Authentication field shows that 802.1x is disabled on VLAN 10, click **Enable** to turn on 802.1x on VLAN 10, and click **Apply** and verify successful operation.
- If 802.1x authentication is to be enabled for IP phones, similarly enable 802.1x on VLAN 100. For this, select **VLAN 100** in this screen, click **Enable**, and the click **Apply**.

Verify from the Properties screen that 802.1x authentication has been enabled on the appropriate VLANs.

Step 6 Select **Security > 802.1x >Port Authentication**.

This displays the Port Authentication screen shown in Figure 6.

Figure 6 Port Authentication Screen



Although 802.1x has been turned on the VLAN(s), this screen allows you to configure it further on a per-port basis. Each port can be configured as one of the following:

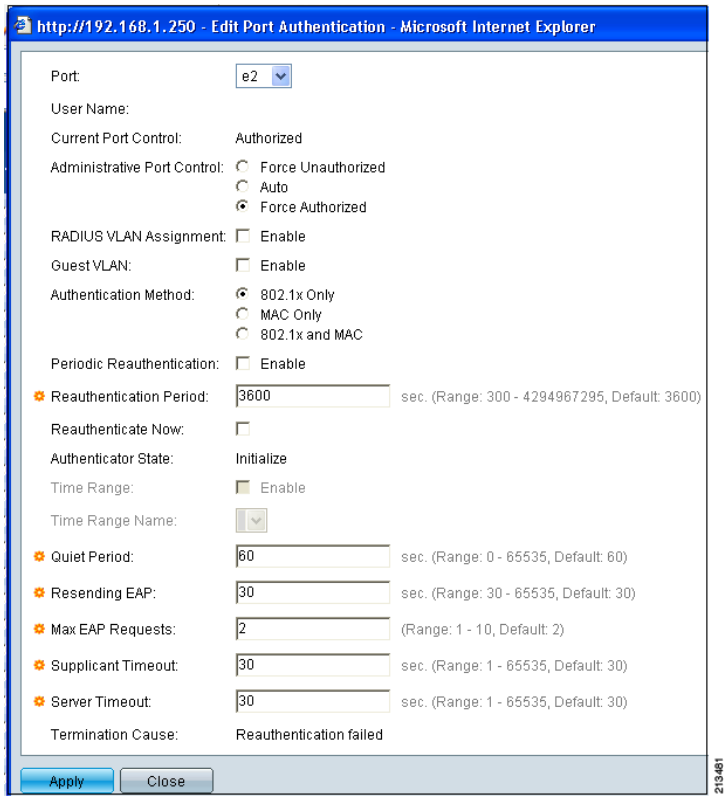
- Force Authorized—Port access is permitted always (turn off 802.1x on this port)
- Force Unauthorized—No access allowed through the port
- Auto—Allows access through the port, only if 802.1x authentication is successful

Although the port should be in Auto mode for 802.1x authentication to take effect, before turning on the mode on the range of ports, you need to configure additional parameters on these ports that require the ports to be in "Forced Authorized" mode. Therefore before proceeding, you need to ensure that the range of ports are in "Forced Authorized" mode.

Step 7 Select port **e2**, and click **Edit**.

This displays the Edit Port Authentication screen shown in Figure 7.

Figure 7 Edit Port Authentication Screen



Step 8 Enter the following values for the fields as shown in Figure 7:

- Administrative Port Control—Select **Force Authorized**.
- Authentication Method—Select **802.1x Only**.
- If required, you may additionally turn on periodic re-authentication. Leave the default values unchanged, as shown in Figure 7.

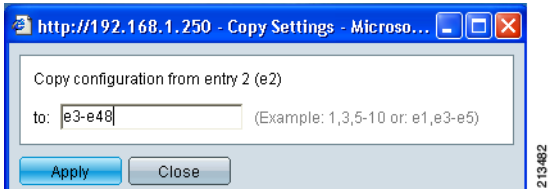
Step 9 Click **Apply**. Verify that "Success" is displayed on the screen.

Step 10 Click **Close** to close the popup screen and display the underlying Port Authentication screen.

Step 11 On the Port Authentication screen, select port **e2**, and click **Copy Settings**.

This displays the Copy Settings popup window shown in Figure 8.

Figure 8 Copy Settings Popup Window



Step 12 Enter the port range (for example, **e3–e48**) to copy the configuration of e2.

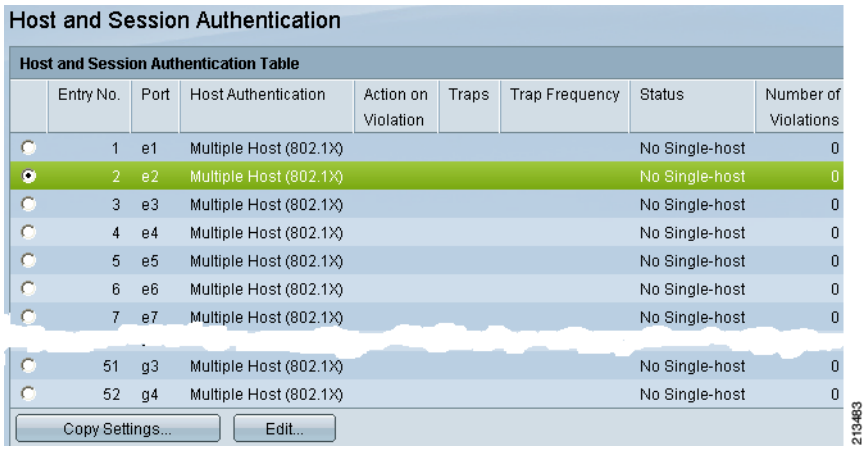
Step 13 Click **Apply**, and verify that the Port Authentication screen displays "Success".

This enables placing the ports in the port range in "Forced Authorized' mode.

Step 14 Select **Security > 802.1x >Hosts and Session Authentication**.

The Host and Session Authentication screen (Figure 9) displays, which allows you to specify access policies to use when more than one device is connected to the port.

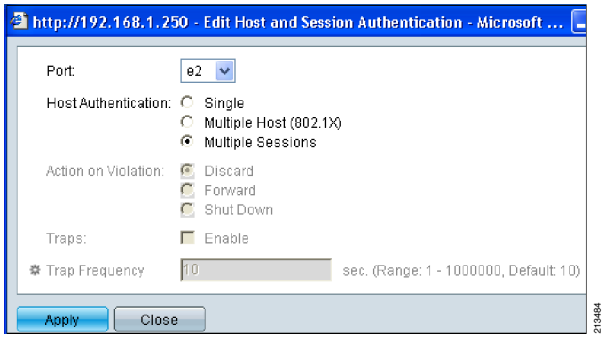
Figure 9 Host and Session Authentication Screen



Step 15 To change the policy on port **e2**, select the port **e2**, as shown in Figure 9, and click **Edit**.

This displays the Edit Hosts and Session Authentication popup screen shown in Figure 10.

Figure 10 Edit Hosts and Session Authentication Popup Screen



Step 16 In the Host Authentication field, select **Multiple Sessions** and click **Apply**.

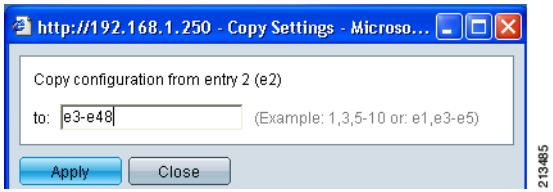
Verify that "Success" is displayed.

If the operation is rejected, go back to Step 7, change the Administrative Port Control field value to **Force Authorized** and try again.

Step 17 On the Host and Session Authentication screen, select port **e2** and click **Copy Settings**.

This displays the Copy Settings popup window shown in Figure 11.

Figure 11 Copy Settings Popup Screen



Step 18 Enter the port range (for example **e3–e48**) to copy the configuration of e2 to the ports specified, and click **Apply**.

Verify that the Host and Session Authentication screen displays "Success".

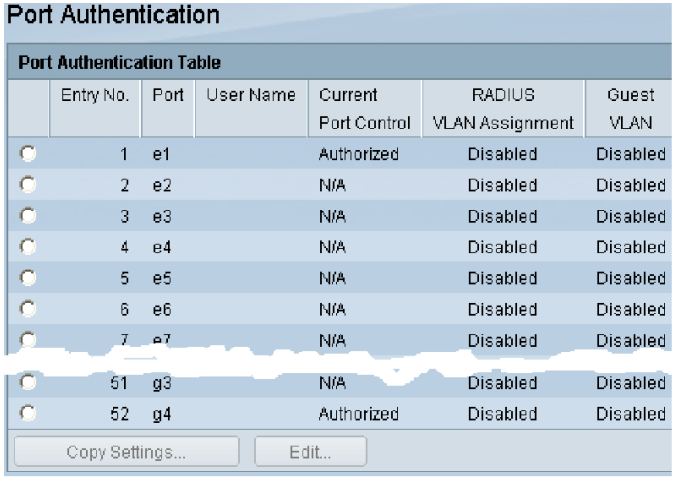
This enables placing the ports in the port range in "Multiple Session" mode of host authentication.

The next step turns on 802.1x authentication on a single port (e2) for verification purposes. After it is verified as working, 802.1.x would be enabled on other ports.

Step 19 To turn on 802.1x authentication on the e2 port, select **Security > 802.1x >Port Authentication**.

The Port Authentication screen is displayed, as shown in Figure 12.

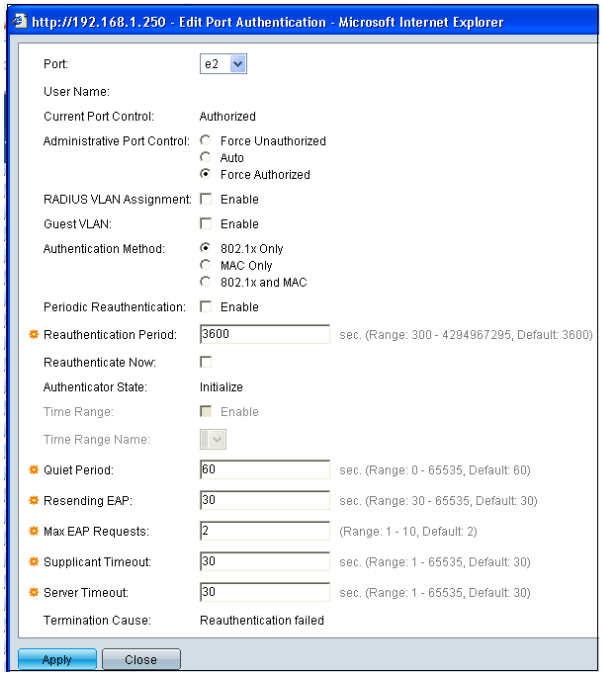
Figure 12 Port Authentication Screen



Step 20 Select port **e2**, and Click **Edit**.

This displays the Edit Port Authentication screen shown in Figure 13.

Figure 13 Edit Port Authentication Screen



Step 21 Enter the following values for the fields:

- Administrative Port Control—Select **Auto**.
- Authentication Method—Select **802.1x Only**
- If required, you may additionally turn on periodic re-authentication. Leave the default values of the timeouts as shown in Figure 13.

Step 22 Click **Apply** and verify that "Success" is displayed on the screen.

Step 23 Click **Close** to close the popup screen and display the underlying Port Authentication screen.

This completes 802.1x configuration on port e2.

Step 24 To verify that 802.1x works on port e2, connect a laptop to the e2 port and configure the laptop's Ethernet connection for the following:

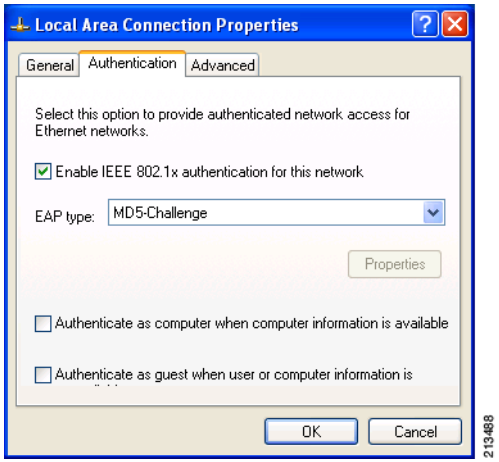
- Accept an IP address and DNS via DHCP
- Perform 802.1x authentication

The exact screens may vary depending on the specific type and version of the laptop OS. The example given here is for Windows XP.

Step 25 Select **Local Area Connection Properties > General > Authentication**.

The screen shown in Figure 14 is displayed.

Figure 14 Local Area Connection Properties—Authentication Tab



Step 26 Check **IEEE 802.1x Authentication**.

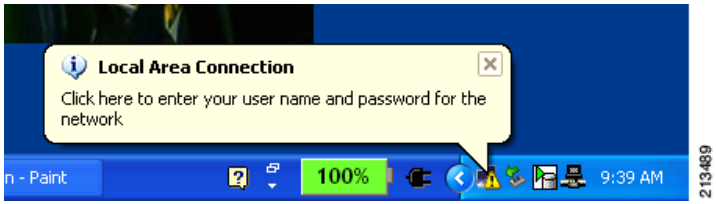
Step 27 Select the EAP type as **MD5-Challenge** or **PEAP** as appropriate.

This must match the type of authentication for the user group configured in the RADIUS server.

Step 28 Click **OK** to save the configuration change.

For a few seconds after connecting the laptop, the laptop may show that the connection is up, although it does not allow access to the user. After a few seconds, a message should appear asking to enter the user name and password, as shown in Figure 15.

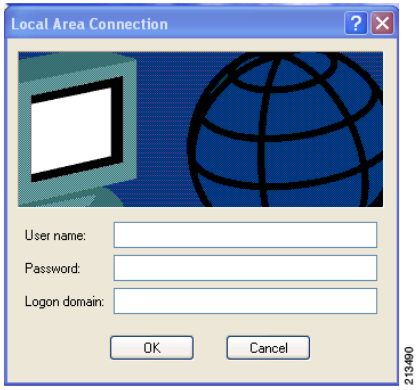
Figure 15 Entering User Name and Password



Step 29 Click the indicated icon.

This displays the screen shown in Figure 16 to enter the user name and password for authentication.

Figure 16 User Authentication Screen



Step 30 Enter the user name and password and click **OK**.

802.1x-based authentication now proceeds to completion, and the laptop's connection icon in the task bar now indicates a successful connection.

Step 31 Select **Security > 802.1x > Port Authentication**.

This displays the Port Authentication screen (Figure 12) with a table that displays the authenticated state of the ports. Verify that port e2 is now listed to be in "Authorized" state under the Current Port Control column.

Step 32 Select **Security > 802.1x > Authenticated Hosts**.

This displays the Authenticated Hosts screen, displaying each port that is currently in 802.1x authenticated state. For each authenticated port, it displays the corresponding user ID, the MAC address of the user device (such as laptop), and session time. Verify that the information displayed here for port e2 are correct.

You can now ping the IP addresses in the network to further verify that the port allows user traffic.

This completes the 802.1x verification on port e2.

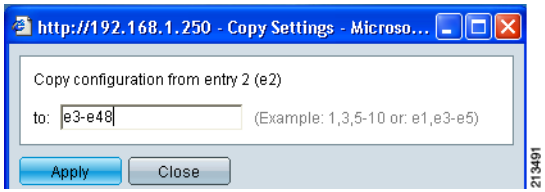
Step 33 To turn on 802.1x authentication on other ports (ports e2–e48, in this example), select **Security > 802.1x >Port Authentication**.

This displays the Port Authentication Screen.

Step 34 Select port **e2**, and click **Copy Settings**.

This displays the Copy Settings popup window shown in Figure 17.

Figure 17 Copy Settings Popup Screen



Step 35 Enter the port range (for example, **e3–e48**) to copy the configuration of e2 to the ports specified, and click **Apply**.

Verify that the Port Authentication screen displays "Success".

This enables 802.1x on the port range specified.

Configuring Time Range-Based Port Access (Optional)

This configuration sets up a port for an absolute time range of 17 Aug, 2010 to 1 Jan, 2020. It also restricts user access to specific periods during each week day (such as from 9 AM to 5 PM on a Monday).

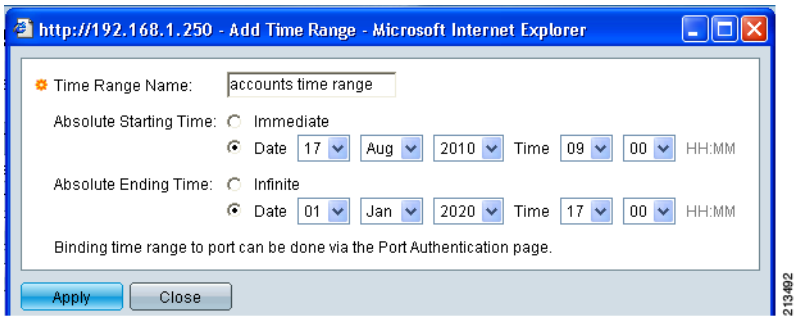
Step 1 Select **Security > 802.1x > Time Range**.

This displays the Time Range screen to add an absolute time range.

Step 2 Click **Add**.

The popup screen shown in Figure 18 is displayed.

Figure 18 Adding Time Range



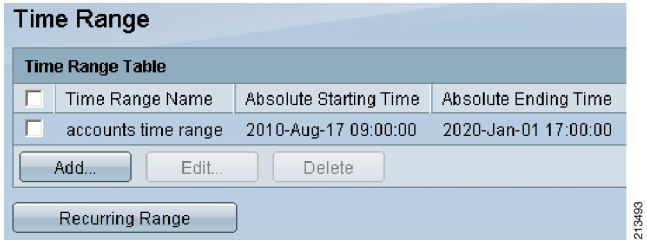
Step 3 Enter a name for the absolute time range (**accounts time range**), and its actual start time, start date, end time, and end date of the time period, as shown in Figure 18.

You may specify the start time as immediate, and/or the end time as infinite, if you like.

Step 4 Click **Apply** and verify that "Success" is displayed.

This displays the screen shown in Figure 19, listing the newly entered time range.

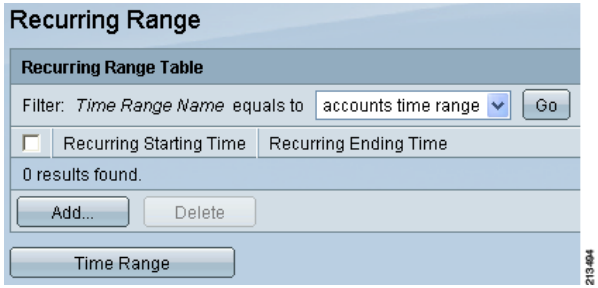
Figure 19 Time Range Screen



Step 5 Click **Recurring Range**.

This displays the Recurring Time Range Screen shown in Figure 20.

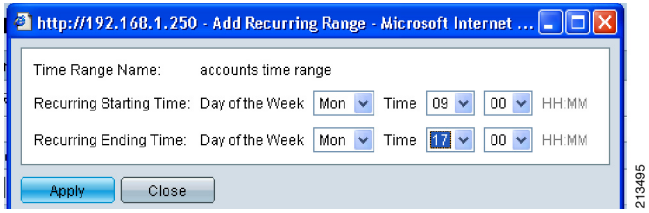
Figure 20 Recurring Range Screen



Step 6 Click **Add...**

This displays the Add Recurring Range screen, as shown in Figure 21, which is used to add one or more recurring time ranges to the selected absolute time range (accounts time range, in this example).

Figure 21 Figure 23



Step 7 Enter Recurring Starting time and Recurring Ending Time values for any single day of the week as shown in Figure 21, and click **Apply**.

Verify that "Success" is displayed.

As shown in Figure 21, this creates a recurring time range for Monday from 9 AM to 5 PM, which allows network access only during this period, provided that 802.1x authentication is successful.

Repeat Steps 5 and 6 to add more recurring time ranges for rest of the days of the week.

This completes the time range creation. Now you need to apply it to the ports.

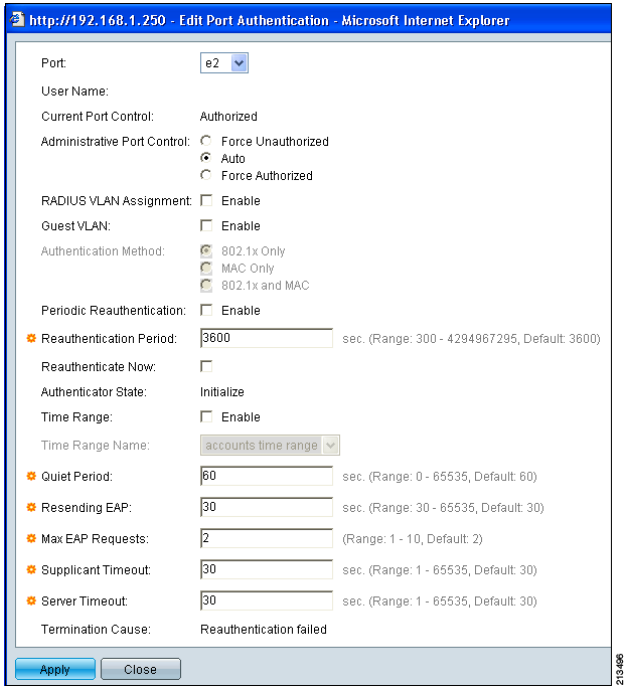
Step 8 Select **Security > 802.1x > Port Authentication**.

This displays the Port Authentication screen listing each port and its details.

Step 9 Select a port (**e2**, in this example) where the time range is to be applied, and click **Edit**.

The screen shown in Figure 22 is displayed with details of the port. Note that the Time Range field is not enabled on this screen by default.

Figure 22 Edit Port Authentication Screen



Step 10 To add the time range to port e2, do the following:

a. Click to enable the Time Range field.

b. In the Time Name Range field, select a time range from the dropdown list (in this case, accounts time range).

Step 11 Click **Apply**.

Verify that the Edit Port Authentication screen displays "Success".

Step 12 Click **Close**, to close the Edit Port Authentication screen.

Port e2 is now configured with the time range.

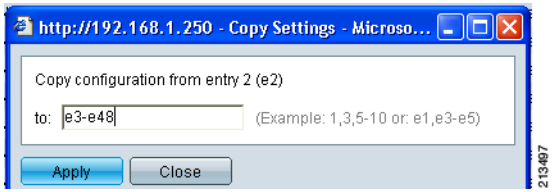
Step 13 Select **Security > 802.1x > Port Authentication**.

This displays the Port Authentication screen listing each port and its details. This allows coping the configuration of port e2 to other similar ports.

Step 14 Select a port (e2, in this example) where the time range has been applied, and click **Copy Settings**.

The screen shown in Figure 23 is displayed to enter the range of ports where the configuration of e2 port will be copied.

Figure 23 Copying Configuration Screen



Step 15 Enter the range (for example, e2–e48) and click **Apply**.

This screen disappears, and the Port Authentication screen is refreshed.

Step 16 Verify that "Success" is displayed on the Port Authentication screen.

This completes 802.1x configuration for the ports e2 through e48.

Summary

This document describes the use of 802.1x authentication and its configuration on a Cisco Small Business 300 Series switch. This enables authenticated access to the LAN ports, thus enhancing network security. To further enhance security, it supports time-based access that further restricts port access to specific ports during specific times of a day. In addition, Dynamic VLAN Assignment can be leveraged to automatically assign the VLAN for a user, so that ports need not be pre-configured with VLANs. These steps make it easier to deploy LANs with greater security and flexibility.

For more information on configuring the Cisco 300 Series Managed Switches, see the Administrator Guide at the following URL:

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