APPLICATION NOTE

No. 330181203-02

Date: **April 2003**
Author: **Eli Shmulenson, ITC Tier IV Product Support Engineering**
Product: **Avaya P330, P330-ML, C460**
General: **Steel-Belted Radius Server configuration for 802.1x support**

Configuring Steel-Belted Radius Server

1. General Description

Steel-Belted Radius server, from Funk Software, is a complete implementation of RADIUS.

RADUIS is an IETF standard security management protocol that lets the network administrator control which LAN users connect to the corporate network, and what resources they can access. It supports port based authentication protocol (IEEE 802.1x) as well as Extended Access Protocol (EAP).

This document is a step-by-step guide to configuring Steel-Belted Radius Enterprise Edition server for Windows NT/2000 to work properly with Avaya P330, P330-ML and C460 switches.

More information about the Steel-Belted Radius server can be found in Funk Software web site: http://www.funk.com.

2. Switch Configuration

Avaya switch configuration is the same for all supported RADIUS servers. There are no definitions specially required for interoperability with Steel-Belted Radius server.

This section describes the CLI commands required to configure Avaya switches to use the RADIUS server for user authentication.

- RADIUS server definition

The following commands define a primary radius server (IP address 149.49.138.113), a shared secret ("test1234") and enable the radius authentication. By default the authentication will be performed using UDP port 1812.

```
P330-1(super)# set radius authentication server 149.49.138.113 primary
P330-1(super)# set radius authentication secret test1234
P330-1(super)# set radius authentication enable
P330-1(super)# show radius authentication
Mode:                 Enable
Primary-server:       149.49.138.113
Secondary-server:     0.0.0.0
Retry-number:         4
Retry-time:           5
UDP-port:             1812
shared-secret:        test1234
```

- 802.1x port-level authentication definition

The following commands define 802.1x authentication and displays authentication status:

```
P330-1(super)# set dot1x system-auth-control enable

dot1x system-auth-control enabled
P330-1(super)# show dot1x
PAE Capabilities             Authenticator Only
Protocol Version             1
system-auth-control          enabled

P330-1(super)# show dot1x
PAE Capabilities             Authenticator Only
Protocol Version             1
system-auth-control          enabled
```

The following command forces authorized authentication for a specific port (usually used for uplink or for the Radius server connection):

```
P330-1(super)# set port dot1x port-control 1/11 force-authorize
```

The following command displays ports authentication status:

```
P330-1(super)# show port dot1x
Port   Auth     BEnd   Port     Port   Re   Quiet ReAuth Server Supp   Tx    Max
Number State    State  Control  Status Auth Priod Priod  Tmeout Tmeout Priod Req
------ -------- ------ -------- ------ ---- ----- ------ ------ ------ ----- ---
 1/1   Connect  Idle   Auto     Unauth Disa    60   3600     30     30    30   2
 1/2   Init     Idle   Auto     Unauth Disa    60   3600     30     30    30   2
 1/3   Init     Idle   Auto     Unauth Disa    60   3600     30     30    30   2
 1/4   Init     Idle   Auto     Unauth Disa    60   3600     30     30    30   2
 1/5   Init     Idle   Auto     Unauth Disa    60   3600     30     30    30   2
 1/6   Init     Idle   Auto     Unauth Disa    60   3600     30     30    30   2
 1/7   Init     Idle   Auto     Unauth Disa    60   3600     30     30    30   2
 1/8   Init     Idle   Auto     Unauth Disa    60   3600     30     30    30   2
 1/9   Init     Idle   Auto     Unauth Disa    60   3600     30     30    30   2
 1/10  Init     Idle   Auto     Unauth Disa    60   3600     30     30    30   2
 1/11  F-Auth   Init   F-Auth   Auth   Disa    60   3600     30     30    30   2
 1/12  Init     Idle   Auto     Unauth Disa    60   3600     30     30    30   2
```

Important notice:

Before enabling the 802.1x authentication support, make sure the switch has IP connectivity to the RADIUS server. If the RADIUS server is connected directly to the switch, make sure its dot1x port-control is in "Force-Authorize" status.

- VLANs definition

Some of the Avaya switches support the feature of applying network parameters to a user port via the Radius server. It is possible to assign a VLAN to a user port (PVID) using Radius attributes. Before doing so, it is required to define all the VLANs that will be used in the system, including those that will be dynamically assigned by the Radius server. Use the "set vlan" command for VLAN definition, as in the following example:

```
P330-1(super)# set vlan 2 name V2
```

Use the "show vlan" command to see all the defined VLANs in the switch.

Important notice:

In P330 family of switches, applying network parameters to a user port by using Radius Server is supported only on 10/100 ports of P334T-ML.

3. **Steel-Belted Radius Server Configuration**

By default, the Steel-Belted Radius server is installed in the C:\Radius\Admin\ directory on the NT/2000-based PC. All the configuration files are installed in C:\Radius\Service\ directory.

3.1 Preparing configuration files

Before running the RADIUS server, you need to modify some of the configuration files. These modifications can be done using any standard text editor, such as Notepad.

- Open the file vendor.ini
- Insert the following line into the vendor.ini file:

```
vendor-product = Avaya
dictionary = Avaya
ignore-ports = no
port-numbering-usage = per-port-type
help-id = 2000
```

- Create a new file avaya.dct in the C:\Radius\Service\ directory containing the following:

```
@radius.dct

ATTRIBUTE Cajun-Service-Type 26 [vid=2167 type1=1 len1=6 data=integer] R
VALUE Cajun-Service-Type Cajun-Read-Only-User 1
VALUE Cajun-Service-Type Cajun-Read-Write-User 2
VALUE Cajun-Service-Type Cajun-Admin-User 3

ATTRIBUTE Avaya-StaticVlan-Type 26 [vid=2167 type1=12 len1=+2 data=string] r
ATTRIBUTE Avaya-PortPriority-Type 26 [vid=2167 type1=13 len1=6 data=integer] R
VALUE Avaya-PortPriority-Type 0 0
VALUE Avaya-PortPriority-Type 1 1
VALUE Avaya-PortPriority-Type 2 2
VALUE Avaya-PortPriority-Type 3 3
VALUE Avaya-PortPriority-Type 4 4
VALUE Avaya-PortPriority-Type 5 5
VALUE Avaya-PortPriority-Type 6 6
VALUE Avaya-PortPriority-Type 7 7
```

- Open the file: dictiona.dcm
- Insert the following line:

```
@avaya.dct
```

- Open the epa.ini file
- Insert the following line in the Native-User section:

```
EAP-Type = TLS, MD5-Challenge
```

- Open the radius.dct file

  The file radius.dct contains all the attributes as defined in standard RADIUS server. You need to change two lines that have to be changed:

```
ATTRIBUTE Tunnel-Private-Group-ID        81  [tag=0 data=string]  R

ATTRIBUTE Tunnel-Type                    64   [tag=0 data=integer]  R
```

Important notice:

After changing the radius configuration files it is required to restart the Steel-Belted radius server. Open the Windows "Services" utility from the Control-Panel (in Windows 2000 it is under Administrative Tools) and restart the Steel-Belted radius daemon.

3.2 Configuring clients and users

After correctly dealing with the radius configuration files, all other radius server definitions can be performed through a GUI based tool – Steel-Belted Radius Administrator. The tool is available trough the Start->Program->Steel Belted Radius menu.

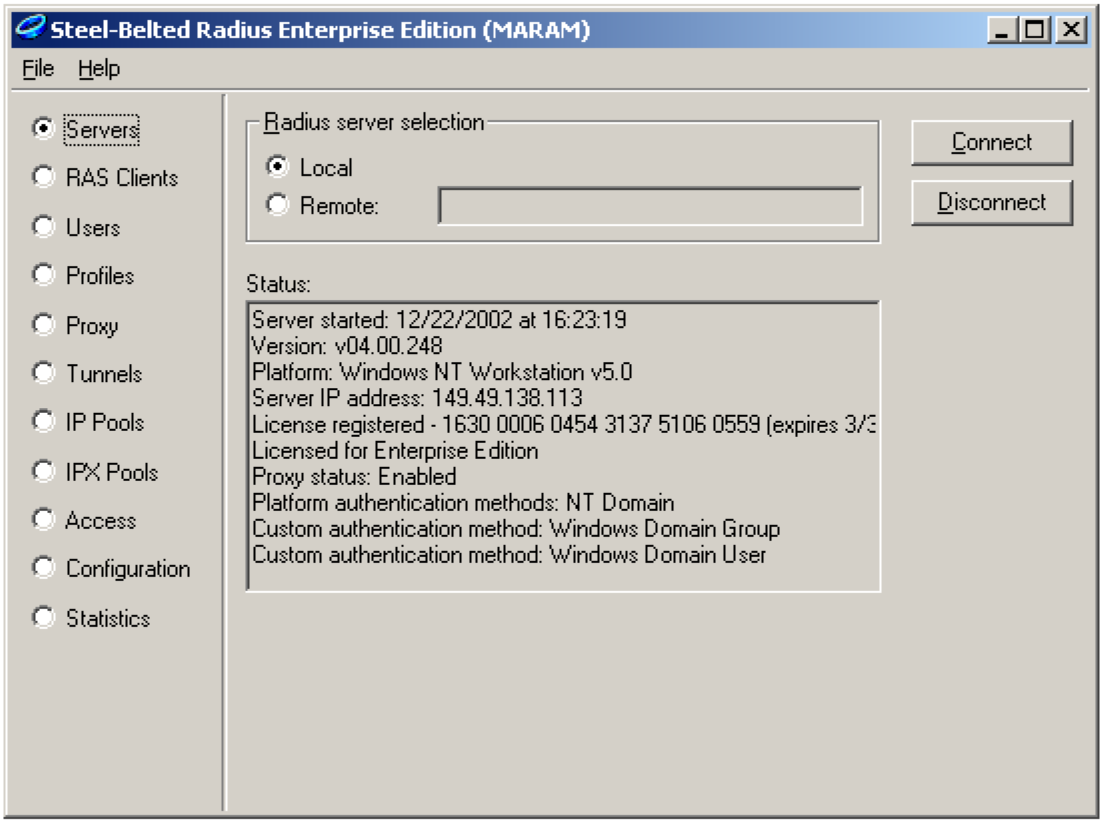
On the left side of the administrator window appear radio buttons for each available section (Servers, RAS Clients, Users, etc). Each section has its own dialog that will appear on the right.

- Connect the administration tool to the radius server

Usually the administration tool is used to configure the RADIUS server that is installed on the local computer. However, there are some cases where the administration tool will be used to configure RADIUS server that is running on a different or remote machine. When you click the "Servers" radio button on the left the "Radius server selection" dialog appears. Since, in our example the administration tool is running on the RADIUS server computer, the selection will be "Local".

Click "Connect" after you made the selection.

The RADIUS server details will appear in the Status section:

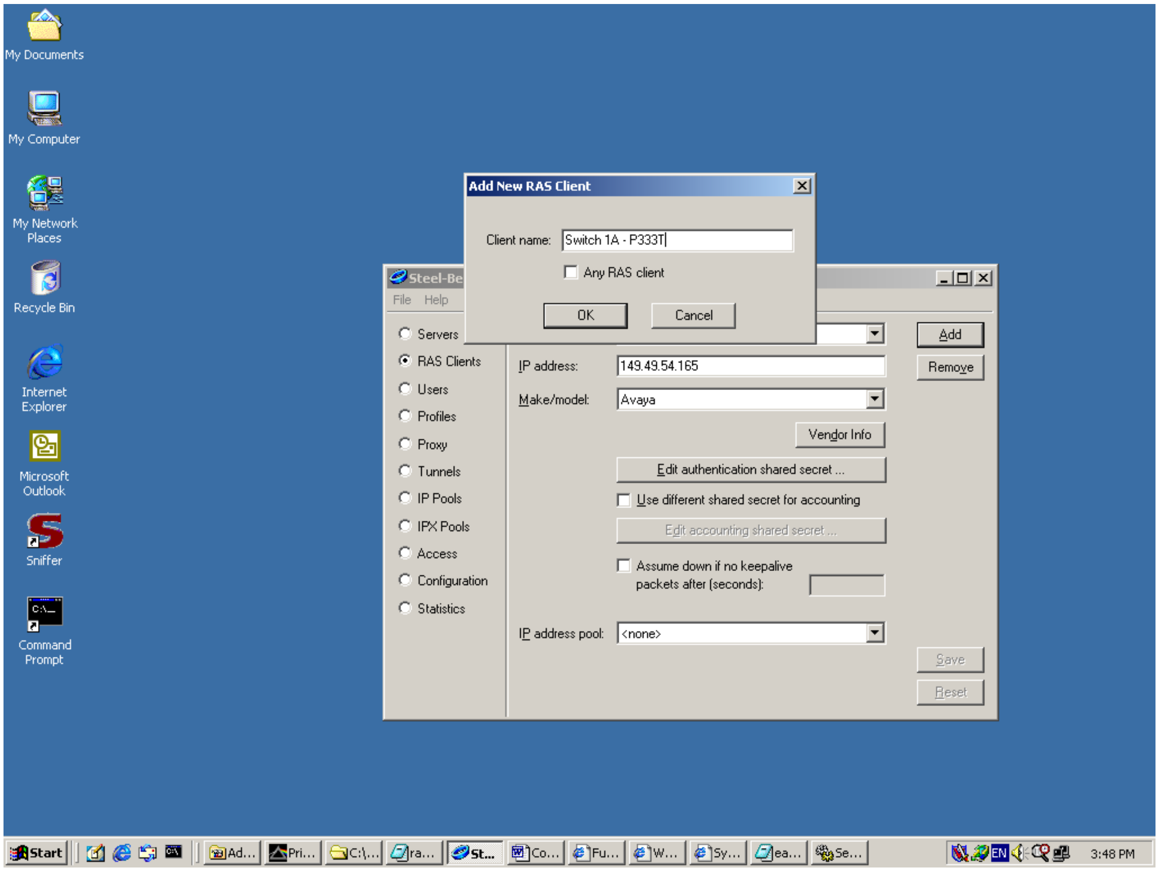


```
Server started: 12/22/2002 at 16:23:19
Version: v04.00.248
Platform: Windows NT Workstation v5.0
Server IP address: 149.49.138.113
License registered - 1630 0006 0454 3137 5106 0559 (expires 3/3
Licensed for Enterprise Edition
Proxy status: Enabled
Platform authentication methods: NT Domain
Custom authentication method: Windows Domain Group
Custom authentication method: Windows Domain User
```

- RAS Clients definition

The RAS Clients dialog lets you identify the devices that you want to be clients of the Steel-Belted Radius server.

Click “Add” button to add a device. Give the device a name and click OK.



Add New RAS Client

Client name: Switch 1A - P333T

□ Any RAS client

OK Cancel

● RAS Clients

IP address: 149.49.54.165

Make/model: Avaya

□ Use different shared secret for accounting

□ Assume down if no keepalive packets after (seconds):

IP address pool: <none>

Enter the device IP address.

Choose “Avaya” in the Make/model drop-down list.

Click “Edit authentication shared secret” and fill in the shared secret *exactly* as defined in the switch RADIUS configuration (section 2 above). Then click “Set”.

Click “Save” to save the RAS Client definition.

Repeat these steps for each network device (RAS Client) in the network.

- Users definition

The Users dialog lets you configure RADIUS authentication details. Each User entry in the Steel-Belted Radius database identifies one method by which the server can authenticate a specific user. The User name field identifies the user; the User type field identifies the method.

In this document we will relate to 2 user types:

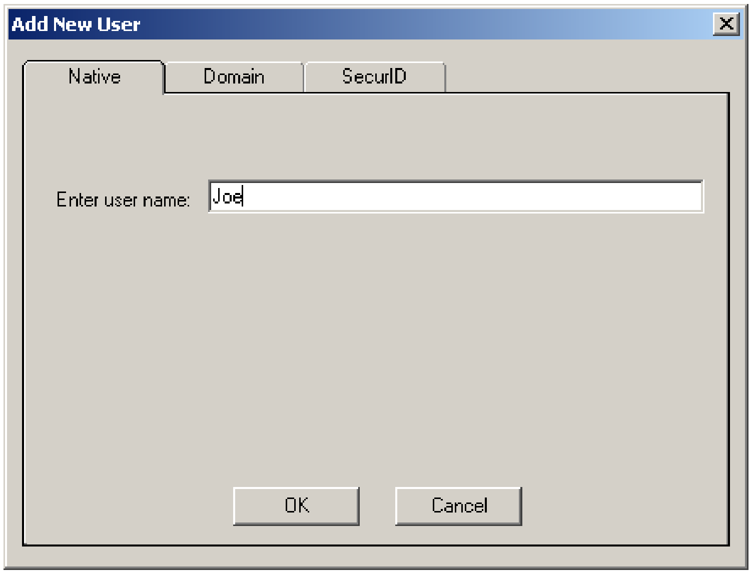
a. Network users, who need to be authenticated in order to use LAN resources.
b. Users who login into the Avaya network devices for maintenance purposes.

Each of the above user types should be defined differently.

a. Network Users definitions:

➢ Step 1 – Adding a user name:

- Click "Add" to add a new user in the Users dialog. An "Add new user" dialog box will appear. Under "Native" bar type the desired user name.



Enter user name: Joe

- Click OK.

- Click "Set Password" to set the password for the user. Leave "Unmask password" checkbox unchecked.

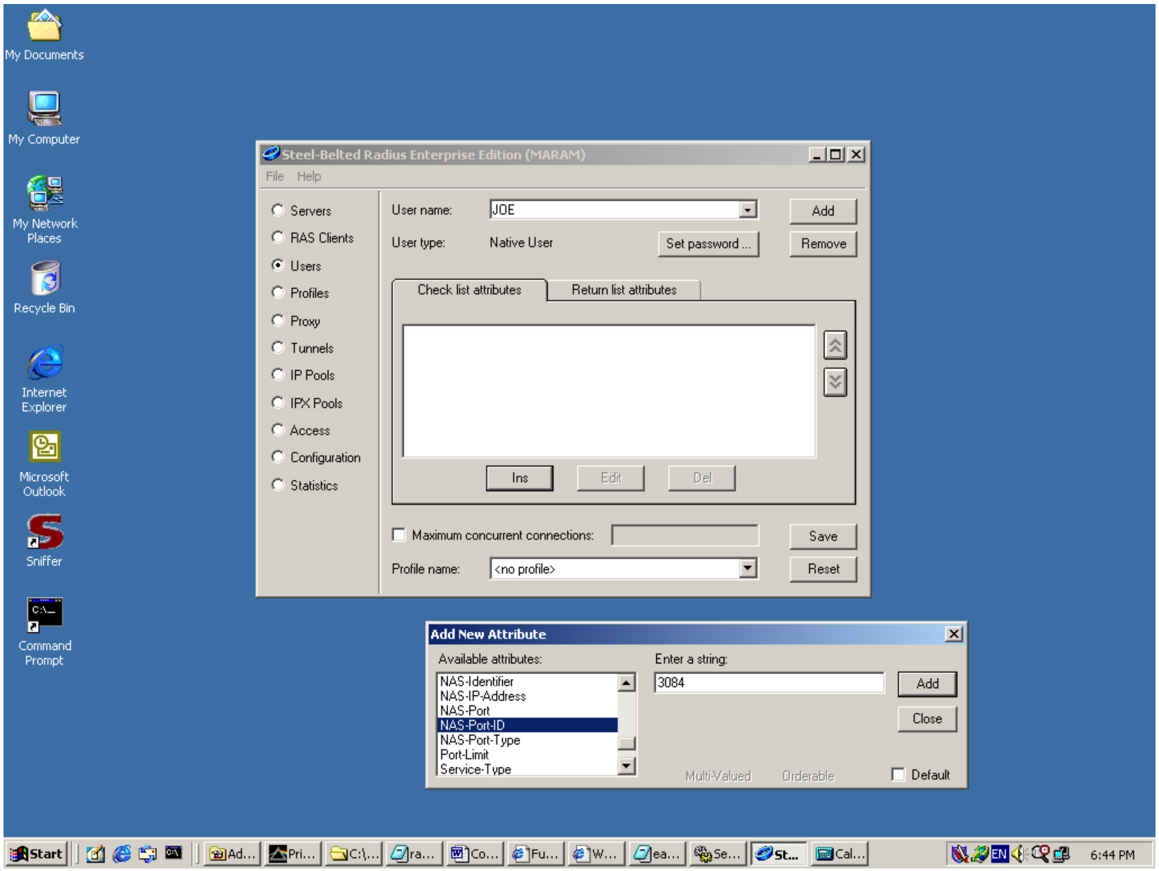
- Select "Allow PAP or CHAP"

- Click “Set”.

➢ Step 2 – User port ID

- Click on “Check list attributes” tab.
- Click “Ins”. An “Add new Attribute” dialog box will appear.
- Select “NAS-Port-ID” from the available attributes bar.

Enter the port number to which the user’s workstation should be connected in the string field. The port number is calculated as following: M*1024+PM stands for module number (in a stack). If the module is stand-alone then M=1.
P represents the physical port number in the module. For example, if there is a stack of 4 switches, while the user is connected to module 3 port 12, then the value should be 3084.



● Users

User name: JOE

User type: Native User

Profile name: <no profile>

Available attributes:
NAS-Identifier
NAS-IP-Address
NAS-Port
NAS-Port-ID
NAS-Port-Type
Port-Limit
Service-Type

Enter a string: 3084

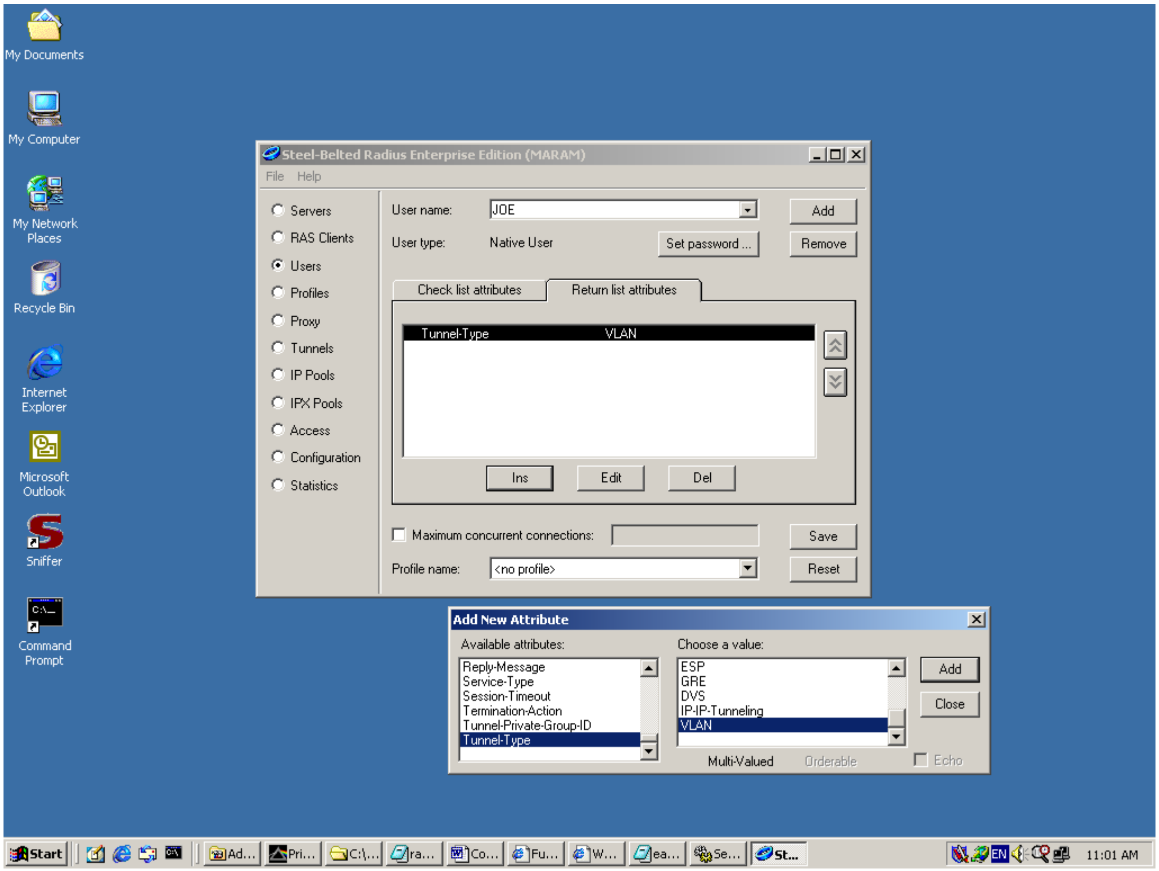
- Click “Add”.
- Click “Close”.

Important notice

The NAS-Port-ID attribute configuration is optional. Not configuring this attribute will cause the radius server to ignore the port number that the user is connected to.

➢ Step 3 – User VLAN number

- Click on "Return list attributes" tab.
- Click "Ins". An "Add new Attribute" dialog box will appear.
- Select "Tunnel-Type" from the available attributes bar.
- Select "VLAN" from the values bar.
- Click "Add".



User name: JOE

User type: Native User

Return list attributes:

Tunnel-Type	VLAN

□ Maximum concurrent connections:

Profile name: <no profile>

Add New Attribute

Available attributes:

- Reply-Message
- Service-Type
- Session-Timeout
- Termination-Action
- Tunnel-Private-Group-ID
- Tunnel-Type

Choose a value:

- ESP
- GRE
- DVS
- IP-IP-Tunneling
- VLAN

Multi-Valued Orderable □ Echo

- Click "Close".

- Click “Ins”. An “Add new Attribute” dialog box will appear.

- Select “Tunnel-Private-Group-ID” from the available attributes bar.

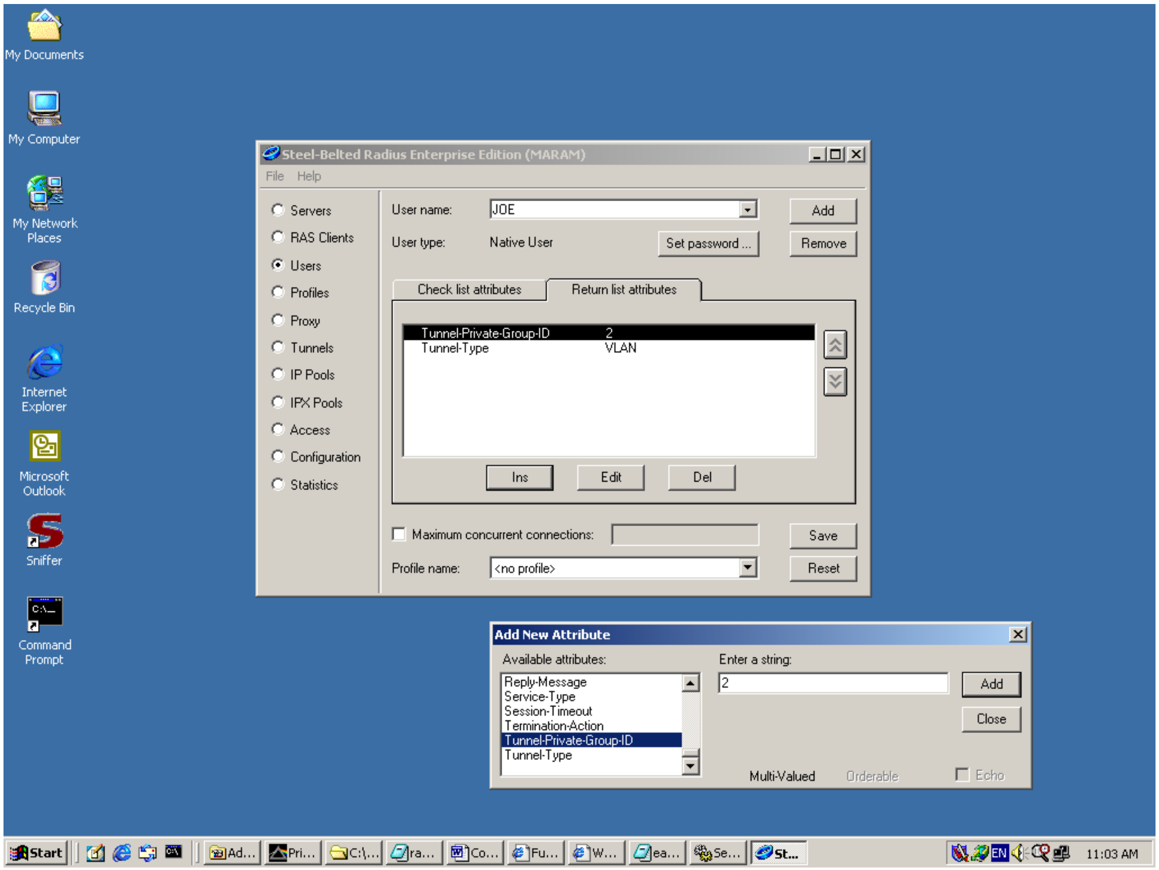
Enter the VLAN number or the VLAN name the user should belong to.

- When the user tries to connect to the network, the radius server will send the value entered to the switch, so the switch will automatically associate the user’s port (set its PVID) to the entered VLAN number/name.

Important notice:

In P330 family of switches, associating VLAN ID to a user port by using Radius Server is supported only on 10/100 ports of P334T-ML.

- Click “Add”.



Steel-Belted Radius Enterprise Edition (MARAM)

User name: JOE

User type: Native User

○ Servers
○ RAS Clients
● Users
○ Profiles
○ Proxy
○ Tunnels
○ IP Pools
○ IPX Pools
○ Access
○ Configuration
○ Statistics

Return list attributes:

Tunnel-Private-Group-ID	2
Tunnel-Type	VLAN

□ Maximum concurrent connections:

Profile name: <no profile>

Add New Attribute

Available attributes:
Reply-Message
Service-Type
Session-Timeout
Termination-Action
Tunnel-Private-Group-ID
Tunnel-Type

Enter a string: 2

Multi-Valued Orderable □ Echo

- Click “Close”.

- Step 4 – Set additional static VLAN for the user

  - Click “Ins”. An “Add new Attribute” dialog box will appear.

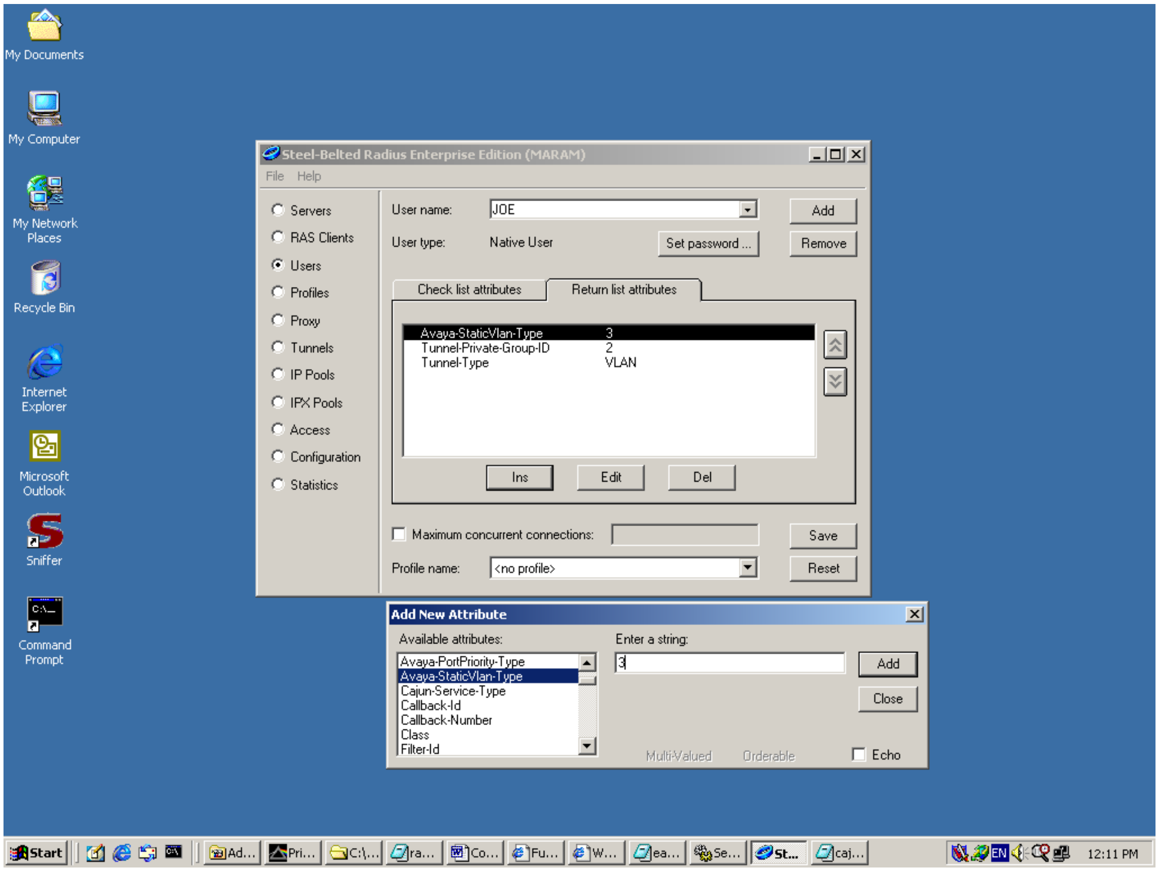
  - Select “Avaya-StaticVlan-Type” from the available attributes bar.

  - Enter an additional VLAN number or the VLAN name the user should belong to. When the user tries to connect to the network, the RADIUS server will send the entered value to the switch, so the switch will automatically statically bind the user’s port to the entered VLAN number/name.

Important notice:

In P330 family of switches, static VLAN binding to a user port by using Radius Server is supported only on 10/100 ports of P334T-ML.

  - Click “Add”.



Steel-Belted Radius Enterprise Edition (MARAM)

○ Servers
○ RAS Clients
● Users
○ Profiles
○ Proxy
○ Tunnels
○ IP Pools
○ IPX Pools
○ Access
○ Configuration
○ Statistics

User name: JOE

User type: Native User

Avaya-StaticVlan-Type	3
Tunnel-Private-Group-ID	2
Tunnel-Type	VLAN

□ Maximum concurrent connections:

Profile name: <no profile>

Add New Attribute

Available attributes:
Avaya-PortPriority-Type
Avaya-StaticVlan-Type
Cajun-Service-Type
Callback-Id
Callback-Number
Class
Filter-Id

Enter a string: 3

□ Echo

  - Click “Close”.

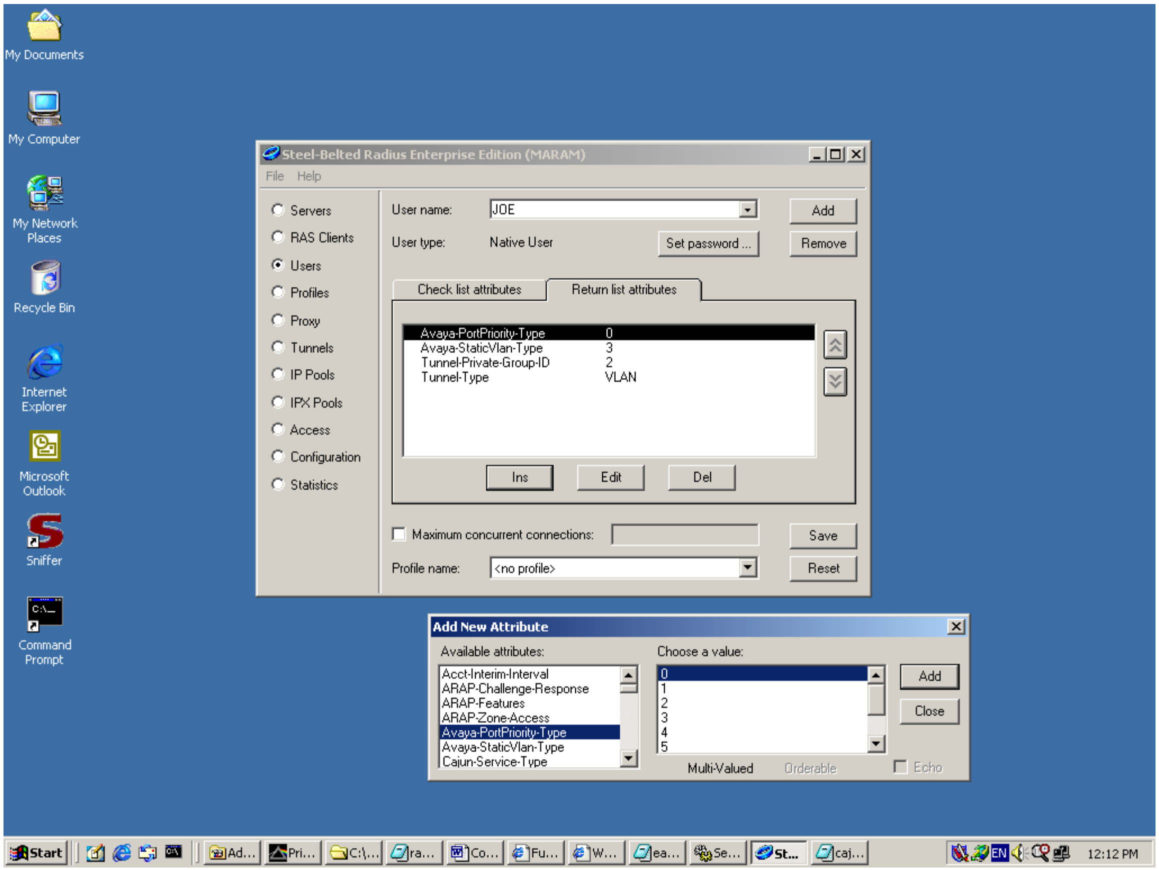
- Step 5 – Set user’s port priority

- Click “Ins”. An “Add new Attribute” dialog box will appear.
- Select “Avaya-PortPriority-Type” from the available attributes bar.
- Choose the desired port priority value for the user. The port priority corresponds to 802.1p eight priority classes (0-7). The switch will set user’s port priority level to the chosen value.

Important notice:

In P330 family of switches, applying priority to a user port by using Radius Server is supported only on 10/100 ports of P334T-ML.

- Click “Add”.



Steel-Belted Radius Enterprise Edition (MARAM)

User name: JOE

User type: Native User

Return list attributes

Avaya-PortPriority-Type	0
Avaya-StaticVlan-Type	3
Tunnel-Private-Group-ID	2
Tunnel-Type	VLAN

□ Maximum concurrent connections:

Profile name: <no profile>

Add New Attribute

Available attributes:

Acct-Interim-Interval
ARAP-Challenge-Response
ARAP-Features
ARAP-Zone-Access
Avaya-PortPriority-Type
Avaya-StaticVlan-Type
Cajun-Service-Type

Choose a value:

0
1
2
3
4
5

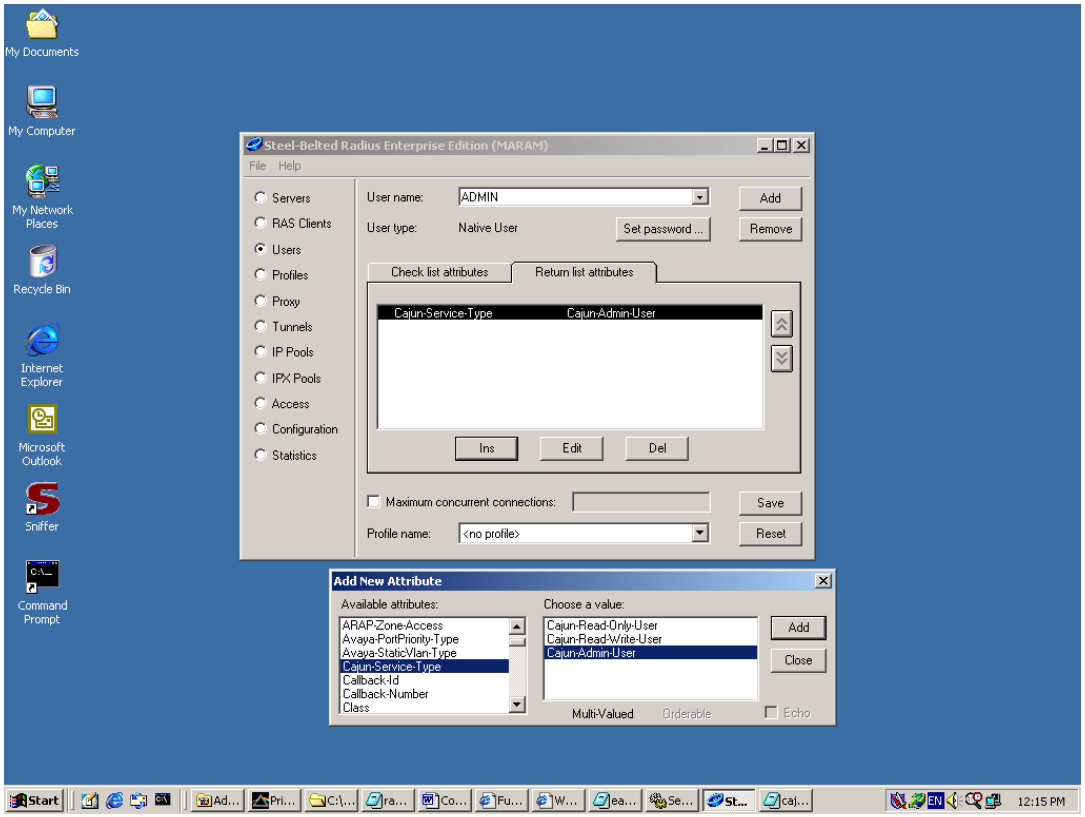
- Click “Close”.

- Step 6 – Saving the user configuration

  - Click “Save”.

b. Switch maintenance users:

- Click “Add” to add a new user in the Users dialog. The “Add new user” dialog box appears.
- Type the desired user name in the “Native” field.
- Click OK.
- Click “Set Password” to set the password for the user. Leave “Unmask password” checkbox unchecked.
- Select “Allow PAP or CHAP”
- Click “Set”.
- Click on “Return list attributes” tab.
- Click “Ins”. The “Add new Attribute” dialog box appears.
- Select “Cajun-Service-Type” from the available attributes drop-down list.
- Choose the desired type of service for the user to have.
- Click “Add”.



○ Servers
○ RAS Clients
● Users
○ Profiles
○ Proxy
○ Tunnels
○ IP Pools
○ IPX Pools
○ Access
○ Configuration
○ Statistics

User name: ADMIN

User type: Native User

Cajun-Service-Type	Cajun-Admin-User

□ Maximum concurrent connections:

Profile name: <no profile>

Available attributes:

- ARAP-Zone-Access
- Avaya-PortPriority-Type
- Avaya-StaticVlan-Type
- Cajun-Service-Type
- Callback-Id
- Callback-Number
- Class

Choose a value:

- Cajun-Read-Only-User
- Cajun-Read-Write-User
- Cajun-Admin-User

Multi-Valued Orderable □ Echo

- Click “Close”.
- Click “Save”.

4. User’s Client Configuration

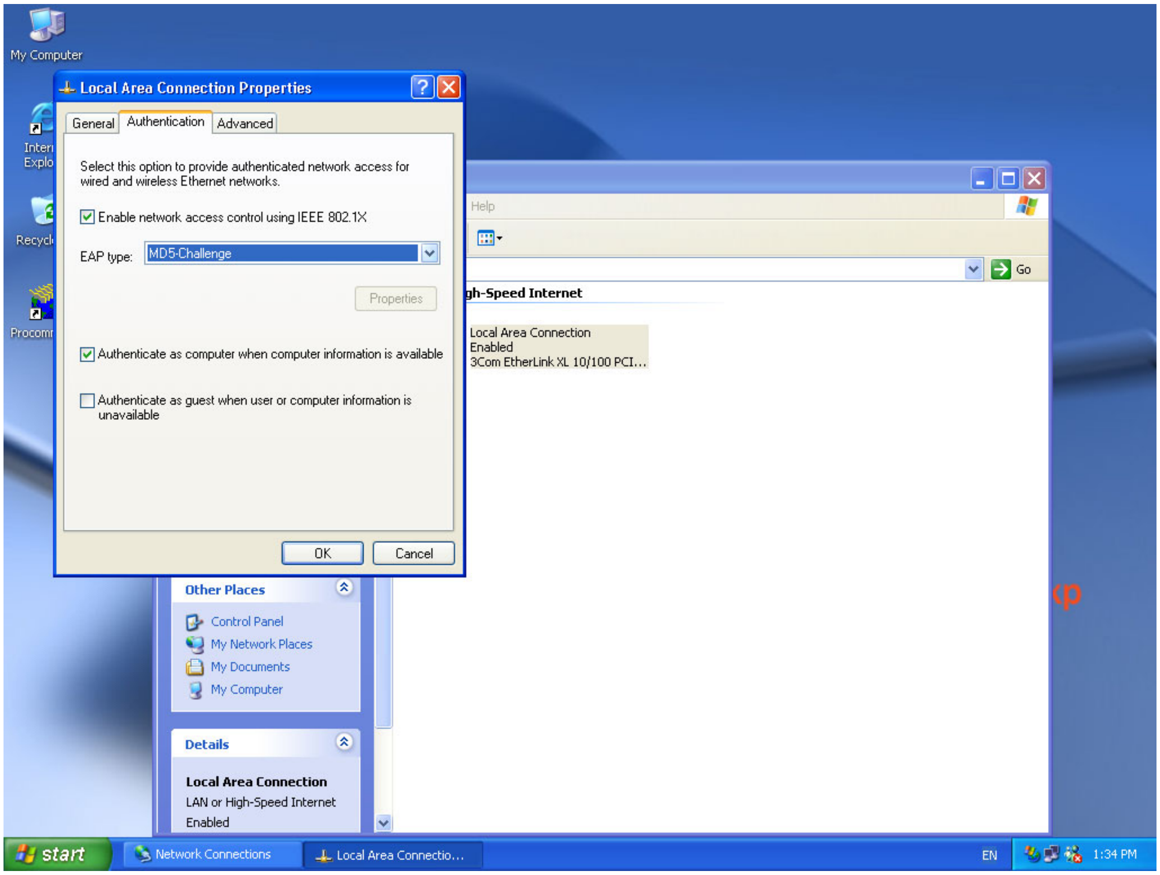
Users who need to login into Avaya switches for maintenance don’t need any special client configuration. During any attempt to login into a switch via Telnet, Web GUI or the console port, a login and password prompt will be displayed. If the user is defined locally in the switch then the switch will grant the user to login. If the user is not locally defined then the switch will refer to the RADIUS server for the authentication.

Network user authentication is performed with client software that supports Extended Access Protocol (EAP). Windows XP has a built-in EAP client for 802.1x port-level authentication. Other operating systems have 3rd party EAP clients.

The following steps describe how to configure Windows XP station for EAP authentication:

- Open the Control Panel.

- Click on “Network and Internet Connections”.
- Click on “Network Connections”.
- Right-click on “Local Area Connection”.
- Select “Properties”.
- Click the “Authentication” tab.
- Check the “Enable network access control using IEEE 802.1X” checkbox.
- In the “EAP type” bar select “MD5-Challenge”.
- Click “OK”.



Local Area Connection Properties

General | Authentication | Advanced

Select this option to provide authenticated network access for wired and wireless Ethernet networks.

☑ Enable network access control using IEEE 802.1X

EAP type: MD5-Challenge

Properties

☑ Authenticate as computer when computer information is available

☐ Authenticate as guest when user or computer information is unavailable

OK | Cancel

As soon as a Windows XP user tries to connect to the network via the configured NIC, a pop-up dialog will guide the user for authentication.