## Content

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Content</td>
<td>2</td>
</tr>
<tr>
<td>Schematic Network Design</td>
<td>4</td>
</tr>
<tr>
<td>Choosing a Microsoft Enterprise Root CA</td>
<td>6</td>
</tr>
<tr>
<td>Standalone CA</td>
<td>6</td>
</tr>
<tr>
<td>Enterprise CA</td>
<td>6</td>
</tr>
<tr>
<td>Configuring Windows Server 2003 Certificate Authority</td>
<td>7</td>
</tr>
<tr>
<td>Install Windows Server 2003 Certificate Authority</td>
<td>7</td>
</tr>
<tr>
<td>Prepare the environment for secure WLAN</td>
<td>11</td>
</tr>
<tr>
<td>Create a group AutoEnroll NPS Server Authentication Certificate</td>
<td>11</td>
</tr>
<tr>
<td>Create a group AutoEnroll Client Authentication – Computer Certificate</td>
<td>11</td>
</tr>
<tr>
<td>Create a group AutoEnroll Client Authentication – User Certificate..... Error! Bookmark not defined.</td>
<td>11</td>
</tr>
<tr>
<td>Configuring and Deploying WLAN Authentication Certificates</td>
<td>16</td>
</tr>
<tr>
<td>NPS Server Authentication</td>
<td>16</td>
</tr>
<tr>
<td>Client Authentication – Computer</td>
<td>19</td>
</tr>
<tr>
<td>Client Authentication – User</td>
<td>22</td>
</tr>
<tr>
<td>Adding Certificate templates to the Certificate Authority</td>
<td>25</td>
</tr>
<tr>
<td>Add NPS Server account to AutoEnroll NPS Server Authentication Certificate group</td>
<td>25</td>
</tr>
<tr>
<td>Create GPOs for Certificate Enrollment</td>
<td>26</td>
</tr>
<tr>
<td>Create a GPO for NPS certificate enrollment</td>
<td>26</td>
</tr>
<tr>
<td>Create a GPO for Client Computer certificate enrollment</td>
<td>27</td>
</tr>
<tr>
<td>Create a GPO for user certificate enrollment</td>
<td>28</td>
</tr>
<tr>
<td>Configuring Network Policy Server</td>
<td>29</td>
</tr>
<tr>
<td>Install Network Policy Server</td>
<td>29</td>
</tr>
<tr>
<td>Register Network Policy Server in Active Directory</td>
<td>32</td>
</tr>
<tr>
<td>Adding RADIUS clients to NPS</td>
<td>32</td>
</tr>
<tr>
<td>Create a Connection Request Policy</td>
<td>33</td>
</tr>
<tr>
<td>Create a Network Request Policy for VLAN 20</td>
<td>37</td>
</tr>
<tr>
<td>Create a Network Request Policy for VLAN 30</td>
<td>41</td>
</tr>
<tr>
<td>Configure DHCP Scopes for wireless access</td>
<td>45</td>
</tr>
<tr>
<td>Configure DHCP Scope for VLAN 20</td>
<td>45</td>
</tr>
<tr>
<td>Configure DHCP Scope for VLAN 30</td>
<td>51</td>
</tr>
<tr>
<td>Configure Cisco Catalyst Switch</td>
<td>56</td>
</tr>
<tr>
<td>Configuring VLANs on the switch</td>
<td>57</td>
</tr>
<tr>
<td>Assigning Switch Ports to VLANs</td>
<td>58</td>
</tr>
<tr>
<td>Configuring Trunk Ports</td>
<td>59</td>
</tr>
<tr>
<td>Configure Cisco Router 2621</td>
<td>60</td>
</tr>
<tr>
<td>Configure the router to support inter-VLAN routing</td>
<td>60</td>
</tr>
<tr>
<td>Configure the wireless access point</td>
<td>61</td>
</tr>
<tr>
<td>Configure the wireless interface Radio0 with a static IP address</td>
<td>62</td>
</tr>
<tr>
<td>Configure IP Settings on the wireless access point</td>
<td>62</td>
</tr>
<tr>
<td>Enable the Radio0 Interface</td>
<td>62</td>
</tr>
<tr>
<td>Define the first wireless network</td>
<td>63</td>
</tr>
<tr>
<td>Define the second wireless network</td>
<td>64</td>
</tr>
<tr>
<td>Configure Encryption Mode for VLAN 20</td>
<td>64</td>
</tr>
</tbody>
</table>
Configure Encryption Mode for VLAN 30 ................................................................. 65
Configure Authentication Method for SCOOBYDOO wireless network ...................... 65
Configure Authentication Method for TWINPEAKS wireless network ....................... 66
Define RADIUS Authentication on the wireless access point ...................................... 67
Define RADIUS Server Priorities .................................................................................. 68
Configure Client Computer for wireless access .......................................................... 69
  Create a wireless network connection for SCOOBYDOO wireless network .................. 69
  Configure Authentication Methods for SCOOBYDOO wireless network ...................... 71
  Connect to SCOOBYDOO wireless network ................................................................ 72
Verify wireless client computer IP address settings ....................................................... 73
Create a wireless network connection for TWINPEAKS wireless network .................... 73
Configure Authentication Methods for TWINPEAKS wireless network ....................... 75
Connect to TWINPEAKS wireless network ................................................................... 76
Verify wireless client computer IP address settings ....................................................... 77
**Purpose**

The purpose of this document is to describe the process how wireless clients can connect to different VLANs on a wireless network.

Today wireless networks contain a single SSID and a static policy associated to each SSID. This means that every user who connects to the wireless network will be granted access based on the policies that you define on the RADIUS server and that every user will retrieve the same settings.

Dynamic VLAN assignment is a feature that places the wireless user into a specific VLAN based on the SSID. This task of assigning users to VLANs is handled by the Network Policy Server on Windows Server 2008. Each wireless network (SSID) can have its own encryption and authentication method. Once the authentication is successful, the Network Policy Server passes some IETF attributes to the user.

The following table gives you a list of the RADIUS attributes used for VLAN assignment:

<table>
<thead>
<tr>
<th>IETF Attribute</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>IETF 64 (Tunnel Type)</td>
<td>Set this to VLAN</td>
</tr>
<tr>
<td>IETF 665 (Tunnel Medium Type)</td>
<td>Set this to 802</td>
</tr>
<tr>
<td>IETF 81 (Tunnel Private Group ID)</td>
<td>Set this to the VLAN ID</td>
</tr>
</tbody>
</table>

**Schematic Network Design**
In this design, VLAN 1 is the native VLAN and VLAN 20, 30 are user-defined VLANs. Only VLAN 20 and 30 are available on the wireless domain.

The following table gives you an overview of all the devices used, their role and IP address:

<table>
<thead>
<tr>
<th>Device</th>
<th>IP Address</th>
<th>VLAN ID</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ADDEVDC01</td>
<td>172.16.10.2</td>
<td>1</td>
<td>Windows Server 2003 Domain Controller, DNS, Enterprise Root CA, DHCP</td>
</tr>
<tr>
<td>ADLHSRV01</td>
<td>172.16.10.3</td>
<td>1</td>
<td>Windows Server 2008 Member Server, Network Policy Server</td>
</tr>
<tr>
<td>ADVI01</td>
<td>Dynamic</td>
<td>Dynamic</td>
<td>Windows Vista Client</td>
</tr>
<tr>
<td>AP</td>
<td>172.16.10.230</td>
<td>1-20-30</td>
<td>Wireless Access Point</td>
</tr>
<tr>
<td>ADDEVRTR</td>
<td>172.16.10.1</td>
<td>1-20-30</td>
<td>Inter-VLAN Router</td>
</tr>
<tr>
<td></td>
<td>172.16.20.1</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>172.16.30.1</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

The following table gives you an overview of the network IDs used in this design:

<table>
<thead>
<tr>
<th>VLAN ID</th>
<th>Network ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>VLAN 1</td>
<td>172.16.10/24</td>
</tr>
<tr>
<td>VLAN 20</td>
<td>172.16.20/24</td>
</tr>
<tr>
<td>VLAN 30</td>
<td>172.16.30/24</td>
</tr>
</tbody>
</table>
Choosing a Microsoft Enterprise Root CA

When you install a Certificate Authority (CA) you have the choice between a Standalone and an Enterprise CA. This means that there are two different policies available how to handle a certificate request.

**Standalone CA**

Standalone CA’s are not integrated in an Active Directory environment and rely on administrative action to verify the user who requests a certificate.

When a user submit a certificate request, the user must apply all identifying information about themselves and the type of certificate the user want to request. By default, all certificate requests send to a standalone CA are set to the pending state, so that a CA administrator can deny or allow the certificate request.

**Enterprise CA**

Enterprise CA’s are integrated with Active Directory and authenticate the user who requests a certificate. This means that the user must have a user account in Active Directory before the user can request a certificate from an Enterprise CA.

When a user logs on, the user has to authenticate them to the domain using a domain user account and password. A domain controller validates the logon request of the user account and is assigned a security token. An Enterprise CA will use this security token to check if the user is allowed to request a certain certificate.

The user can manually request a certificate by using the users’ web browser or a CA administrator can assign auto-enrollment via Group Policies. A CA administrator also can configure an Enterprise CA so that a computer account can automatically receive a certificate. This process is also done via Group Policies.
When a computer starts up, a list of previously assigned computer certificates is compared with the certificate templates assigned via Group Policies. If the computer does not have a valid certificate for an assigned certificate template, the computer will request the certificate.

An Enterprise CA works with certificate templates. A certificate template identifies a certificate because there are some purposes defined in these templates for what the certificate actually can be used. Additionally a CA administrator has to modify the Discretionary Access List (DACL) to assign permissions to certificate templates.

### Configuring Windows Server 2003 Certificate Authority

- Install Windows Server 2003 Certificate Authority

#### Install Windows Server 2003 Certificate Authority

- Open **Add or Remove Programs** from the **Control Panel**.
- Click on **Add/Remove Windows Components** and select **Certificate Services** from the **Windows Components Wizard** dialog box and click **Next**.
- Select **Certificate Services** and on the Microsoft Certificate Services exclamation box, click **Yes**.
- On the **Certificate Authority Type** page, select the appropriate type of CA you want to set up and click **Next**.
On the **CA Identifying Information** page, enter information that is appropriate for your company in the **Common name** for this CA textbox and specify also the **Validity period** for CA certificate, click **Next**.

On the **Certificate Database Settings** page, enter location for the certificate database, database log and configuration information, click **Next**.
A **Configuring Components** page shows up to display setup information.

- Click **Finish** to exit the installation process.
Note: If you want to change the default cryptographic settings, select the Use custom settings to generate the key pair and CA certificate. Then you will be prompted to change the CSP, hash algorithm and key length.

If you setup a CA from an earlier version or if you had previously a standalone CA and you want to move to an enterprise CA, then you have to select this checkbox and select Use an existing key from the dialog box.
Prepare the environment for secure WLAN

You need to prepare the environment with wireless groups to support the appropriate authentication. The next step is the create security groups in Active Directory for wireless access.

- Create a group AutoEnroll NPS Server Authentication Certificate
- Create a group AutoEnroll Client Authentication – Computer Certificate
- Create a user account for VLAN 20
- Create a user account for VLAN 30
- Create a group Wireless Users VLAN 20
- Create a group Wireless Users VLAN 30

Create a group AutoEnroll NPS Server Authentication Certificate

- Open Active Directory Users and Computers from Administrative Tools.
- Select Organization Unit you want to create the group.
- Right click on the OU, select New – Group
- On the New Object – Group window, type the name of the group AutoEnroll NPS Server Authentication Certificate and click OK

Create a group AutoEnroll Client Authentication – Computer Certificate

- Open Active Directory Users and Computers from Administrative Tools.
- Select Organization Unit you want to create the group.
Right click on the OU, select **New – Group**

On the **New Object – Group** window, type the name of the group *AutoEnroll Client Authentication - Computer Certificate* and click **OK**

Create a user account for VLAN 20

- Open **Active Directory Users and Computers** from **Administrative Tools**.
- Select Organization Unit you want to create the user.
- Right click on the OU, select **New – User**
- On the **New Object – User** dialog box, type *Stef* in **First Name** and type *Stef* in **User Logon Name**. Click **Next**
In the New Object – User dialog box, type a password of your choice in Password and Confirm Password box. Clear User must change password at next logon check box. Click Next and click Finish.

Create a user account for VLAN 30

- Open Active Directory Users and Computers from Administrative Tools.
- Select Organization Unit you want to create the user.
Right click on the OU, select **New – User**

On the **New Object – User** dialog box, type *Johan* in **First Name** and type *Johan* in **User Logon Name**. Click **Next**

In the **New Object – User** dialog box, type a password of your choice in **Password** and **Confirm Password** box. Clear **User must change password at next logon** check box. Click **Next** and click **Finish**.

**Create a group Wireless Users VLAN 20**
Open **Active Directory Users and Computers** from **Administrative Tools**.
Select Organization Unit you want to create the group.
Right click on the OU, select **New – Group**
On the **New Object – Group** window, type the name of the group **Wireless Users VLAN 20** and click **OK**

In the details pane, double click on Wireless Users VLAN 20.
Click on the **Members** tab and click **Add**.
On the **Select Users, Contact, Computers, or Groups** dialog box, in the **Enter the object names to select**, type Stef and click **OK**

**Create a group Wireless Users VLAN 30**
Open **Active Directory Users and Computers** from **Administrative Tools**.
Select Organization Unit you want to create the group.
Right click on the OU, select **New – Group**
On the **New Object – Group** window, type the name of the group **Wireless Users VLAN 30** and click **OK**
In the details pane, double click on Wireless Users VLAN 20.

Click on the Members tab and click Add.

On the Select Users, Contact, Computers, or Groups dialog box, in the Enter the object names to select, type Johan and click OK.

**Configuring and Deploying WLAN Authentication Certificates**

Before we can use the wireless network, we need to deploy certificates. In this section, you need to create and deploy following certificate templates.

- NPS Server Authentication
- Client Authentication – Computer
- Client Authentication – User
- Adding Certificate templates to the Certificate Authority
- Add NPS Server account to AutoEnroll NPS Server Authentication Certificate group
- Add Client computer account to AutoEnroll Client Authentication - Computer Certificate group

**NPS Server Authentication**

A server certificate is required on the NPS server to authenticate the wireless client computers during the EAP-TLS protocol handshake.
Open **Certificate Authority** from **Administrative Tools**.
- Right click on **Certificate Templates** and select **Manage**.
- Right click on **RAS and IAS Server certificate template** and select **Duplicate Template**.
- On the **General** tab, in the Template display name field, type **NPS Server Authentication**.

![Certificate Authority Configuration](image)

- Click on the **Subject Name** tab, select **Build from this Active Directory information**. Ensure that the subject name format is set to **Common name** and that only **DNS Name** is selected under **Include this information in subject alternative name**.
- Click on the **Security** tab, click on the **Add** button and add *AutoEnroll NPS Server Authentication Certificate* group. Assign **Enroll** and **Autoenroll** permissions and click **OK**.
Note: You should remove RAS and IAS Servers from the ACL.

**Client Authentication – Computer**

- Open **Certificate Authority** from **Administrative Tools**.
- Right click on **Certificate Templates** and select **Manage**.
- Right click on **Workstation Authentication** certificate template and select **Duplicate Template**.
- On the **General** tab, in the Template display name field, type *Client Authentication - Computer*. 
Click on the **Subject Name** tab, select **Build from this Active Directory information**. Ensure that the subject name format is set to **Common name** and that only **DNS Name** is selected under **Include this information in subject alternative name**.
Click on the **Security** tab, next click on the **Add** button and add *AutoEnroll Client Authentication – Computer Certificate* group. Assign **Enroll** and **Autoenroll** permissions and click **OK**.
Configuring wireless dynamic VLANs on Windows Server 2008, version 1.0

Client Authentication – User

- Open Certificate Authority from Administrative Tools.
- Right click on Certificate Templates and select Manage.
- Right click on User certificate template and select Duplicate Template.
- On the General tab, in the Template display name field, type Client Authentication - User.

Note: You should remove the Domain Computers group from the ACL.
Click on the **Subject Name** tab, select **Build from this Active Directory information**. Under Subject name format, select **Fully distinguished name**. Ensure that **User Principal Name (UPN)** is the only option select under **Include this information in subject alternative name**.

- Verify that **Include e-mail name in subject name** and **E-mail name** boxes are cleared.
Click on the **Security** tab, next click on the **Add** button and add *Wireless Users VLAN 20* and *Wireless Users VLAN 30* groups. Assign **Enroll** and **Autoenroll** permissions and click **OK**.
Note: You should remove the Domain Users group from the member list.

**Adding Certificate templates to the Certificate Authority**

After you have configured or created new certificate templates, you have to add them to the certificate authority to enable enrollment.

- From the **Certificate Authority**, right click on **Certificate Templates**, select **New – Certificate Template to Issue**.
- Select following certificate templates: Client Authentication – Computer, Client Authentication – User, NPS Server Authentication and click **OK**.
- Close Certificate Authority snap-in.

**Add NPS Server account to AutoEnroll NPS Server Authentication Certificate group**

- Open **Active Directory Users and Computers** from **Administrative Tools**.
- Double click on the **AutoEnroll NPS Server Authentication Certificate** group.
Select **Members** tab, click on the **Add** button. Add NPS computer account and click **OK**.

**Add Client computer account to AutoEnroll Client Authentication – Computer Certificate group**

- Open **Active Directory Users and Computers** from **Administrative Tools**.
- Double click on the **AutoEnroll Client Authentication -Computer Certificate** group.
- Select **Members** tab, click on the **Add** button. Add the client computer account and click **OK**.

**Create GPOs for Certificate Enrollment**

- Create a GPO for NPS certificate enrollment
- Create a GPO for Client Computer certificate enrollment
- Create a GPO for user certificate enrollment

**Create a GPO for NPS certificate enrollment**

- Open **Group Policy Management Console** from **Administrative Tools**.
- Expand Domains, right click on **Group Policy Objects**, select **New** and type **GPO NPS Server** and click **OK**.
- Right click on GPO NPS Server Authentication and select **Edit**
- In the details pane, double click on **Autoenrollment Settings**.
- Click **Enroll certificates automatically**. Select **Renew expired certificates**, **update pending certificates**, and **remove revoked certificates** check box.
- Select the **Update certificates that use certificate templates** check box and click **OK**.
Close Group Policy Editor

- Click on the Details tab, select User Configuration Settings Disabled from the GPO Status list box.
- Link the GPO to the appropriate OU.
- On the NPS server, open command prompt and execute gpupdate.exe

Create a GPO for Client Computer certificate enrollment

- Open Group Policy Management Console from Administrative Tools.
- Expand Domains, right click on Group Policy Objects, select New and type GPO Client Authentication – Computer and click OK.
- Right click on GPO Client Authentication and select Edit
- In the details pane, double click on Autoenrollment Settings.
- Click Enroll certificates automatically. Select Renew expired certificates, update pending certificates, and remove revoked certificates check box.
- Select the Update certificates that use certificate templates check box and click OK.
Close Group Policy Edit
- Click on the Details tab, select User Configuration Settings Disabled from the GPO Status list box.
- Link the GPO to the appropriate OU.
- On the client computer, open command prompt and execute gpupdate.exe

Create a GPO for User certificate enrollment
- Open Group Policy Management Console from Administrative Tools.
- Expand Domains, right click on Group Policy Objects, select New and type GPO Client Authentication – User, click OK.
- Right click on GPO Client Authentication - User and select Edit
- In the details pane, double click on Autoenrollment Settings.
- Click Enroll certificates automatically. Select Renew expired certificates, update pending certificates, and remove revoked certificates check box.
- Select the Update certificates that use certificate templates check box and click OK.
Close Group Policy Edit.

Click on the Details tab, select Computer Configuration Settings Disabled from the GPO Status list box.

Link the GPO to the appropriate OU.

On the client computer, open command prompt and execute gpupdate.exe

---

**Configuring Network Policy Server**

- Install Network Policy Server
- Register Network Policy Server in Active Directory
- Adding RADIUS clients to NPS
- Create a Connection Request Policy
- Create a Network Request Policy for VLAN 20
- Create a Network Request Policy for VLAN 30

**Install Network Policy Server**

- On Server Manager, select Add Roles.
On the **Network Policy and Access Services** page, select **Next**.

On the **Select Role Services** page, select **Network Policy Server** and click **Next**.
On the **Confirm Installation Selection** page, select **Install**.

On the **Installation Result** page, select **Close**.
Register Network Policy Server in Active Directory

- Open Network Policy Server from Administrative Tools.
- Right click on NPS(local) and select Register Server in Active Directory.

Adding RADIUS clients to NPS

- Open Network Policy Server from Administrative Tools.
- Expand RADIUS Clients and Servers, right click on RADIUS client and select New RADIUS Client.
- On the New RADIUS Client page, specify a friendly name and Address. Specify a Vendor name. Also specify a Shared secret and select Access-Request messages must contain the Message-Authenticator Attribute under Additional Options and click OK.
Create a Connection Request Policy

- Open **Network Policy Server** from **Administrative Tools**
- Expand Policies, right click on **Connection Request Policies** and select **New**.
- On the **Specify Connection Request Policy Name and Connection Type** page, specify a Policy name **Secure Wireless Access** and click **Next**
On the **Policy Conditions** page, click **Add**, select **NAS Port Type** and click **Add**. On the **NAS Port Type** dialog box, select **Wireless IEEE 802.11** and click **OK**.

- Click **Next**.
On the **Specify Connection Request Forwarding** page, select **Next**.

On the **Specify Authentication Methods** page click **Next**.
On the **Configure Settings** page, accept defaults and click **Next**.

On the **Completing Connection Request Policy Wizard** page, click **Finish**.
Create a Network Request Policy for VLAN 20

- Open **Network Policy Server** from **Administrative Tools**.
- Expand Policies, right click on **Network Policies** and select **New**.
- On the **Specify Network Policy Name and Connection Type** page, specify a Policy Name **Wireless Users – VLAN 20** and click **Next**.
On the **Specify Conditions** page, click **Add**. On the **Select Condition** dialog box, select Windows Groups and click **Add**. On the **Windows Group** dialog box, click **Add Groups** and add Wireless User VLAN 20 group and click **OK**.

On the **Specify Conditions** page, click **Add**. Select **NAS Port Type** and click **Add**. On the **NAS Port Type** dialog box, under **Common 802.1x connection tunnel types**, select **Wireless-IEEE 802.11**. Click **OK** and click **Next**.

On the **Specify Access Permissions** page, select **Access Granted** and click **Next**.
On the **Authentication Methods** page, click **Add**. On the **Add EAP** dialog box, select **Microsoft: Smart Card or Certificate** and click **OK**. Clear all other authentication methods and click **Next**.

On the **Configure Constraints** page, click **Next**.
On the **Configure Settings** page, select **RADIUS Attributes-Standard**. Click **Add** as seen below and click **Next**.

- Tunnel-Type: VLAN
- Tunnel-Pvt-Group-ID: 20
- Tunnel-Medium-Type: 802

On the **Completing New Network Policy** page, select **Finish**.
Create a Network Request Policy for VLAN 30

- Open Network Policy Server from Administrative Tools.
- Expand Policies, right click on Network Policies and select New.
- On the Specify Network Policy Name and Connection Type page, specify a Policy Name Wireless Users – VLAN 30 and click Next.
On the **Specify Conditions** page, click **Add**. On the **Select Condition** dialog box, select **Windows Groups** and click **Add**. On the **Windows Group** dialog box, click **Add Groups** and add Wireless User VLAN 30 group and click **OK**.

On the **Specify Conditions** page, click **Add**. Select **NAS Port Type** and click **Add**. On the **NAS Port Type** dialog box, under **Common 802.1x connection tunnel types**, select **Wireless-IEEE 802.11**. Click **OK** and click **Next**.

On the **Specify Access Permissions** page, select **Access Granted** and click **Next**.
On the Authentication Methods page, click Add. On the Add EAP dialog box, select Microsoft: Smart Card or Certificate and click OK. Click Next.

On the Configure Constraints page, click Next.
On the **Configure Settings** page, select **RADIUS Attributes-Standard**. Click **Add** as seen below and click **Next**.

- Tunnel-Type: VLAN
- Tunnel-Pvt-Group-ID: 30
- Tunnel-Medium-Type: 802

On the **Completing New Network Policy** page, select **Finish**.
Configure DHCP Scopes for wireless access

- Configure DHCP Scope for VLAN 20
- Configure DHCP Scope for VLAN 30

**Configure DHCP Scope for VLAN 20**

- Open **DHCP Console** from **Administrative Tools**.
- Right click on DHCP Server and select **New Scope**.
- On the **Welcome** page, click **Next**.
On the **Scope Name** page, type a name of the scope and click **Next**.

On the **IP Address Range** page, specify the Start and End IP address and click **Next**.
On the **Address Exclusions** page, click **Next**.

On the **Lease Duration** page, specify the lease duration of 1 hour and click **Next**.
On the **Configure DHCP Options** page, select **Yes, I want to configure these options now** and click **Next**.

On the **Router** page, type the IP address of the router 172.16.20.1, click **Add** and click **Next**.
On the Domain Name and DNS Servers page, specify the domain name and IP address of the DNS server. Click Add and click Next.

On the WINS Servers page, click Next.
On the **Active Scope** page, select **Yes, I want to activate this scope now**, click **Next**.

On the **Completing** page, click **Finish**.
Configure DHCP Scope for VLAN 30

- Open DHCP Console from Administrative Tools.
- Right click on DHCP Server and select New Scope.
- On the Welcome page, click Next.

- On the Scope Name page, type a name of the scope and click Next.
On the **IP Address Range** page, specify the Start and End IP address and click **Next**.

On the **Address Exclusions** page, click **Next**.
On the **Lease Duration** page, specify the lease duration of 1 hour and click **Next**.

On the **Configure DHCP Options** page, select **Yes, I want to configure these options now** and click **Next**.
On the **Router** page, type the IP address of the router 172.16.30.1 click **Add** and click **Next**.

On the **Domain Name and DNS Servers** page, specify the domain name and IP address of the DNS server. Click **Add** and click **Next**.
On the WINS Servers page, click Next.

On the Active Scope page, select Yes, I want to activate this scope now, click Next.
On the Completing page, click Finish.

Configure Cisco Catalyst Switch

When you use an IEEE 802.1Q trunk port, all frames are tagged except those on the VLAN configured as the native VLAN for the port. Frames on the native VLAN are always transmitted and received untagged.

When you configure the switch, ensure that all VLANs that are configured on the wireless access point are allowed on the switchport.
By default, a switchport configured as trunk allows all VLANs to pass through the trunk. This can become a performance problem, which result in a high CPU utilization on the wireless access point.

- Overview of the switch layout
- Configuring VLANs on the switch
- Assigning Switch Ports to VLANs
- Configuring Trunk Ports

**Overview of the switch layout**

On the following table, you can find which switch ports are configured and which device is connected to which switch port.

<table>
<thead>
<tr>
<th>Switch Port</th>
<th>VLAN ID</th>
<th>Status</th>
<th>Port Mode</th>
<th>Device</th>
</tr>
</thead>
<tbody>
<tr>
<td>fa 0/1</td>
<td>1</td>
<td>Used</td>
<td>trunk</td>
<td>ADBERTR01</td>
</tr>
<tr>
<td>fa 0/2</td>
<td>1</td>
<td>Used</td>
<td>trunk</td>
<td>AP</td>
</tr>
<tr>
<td>fa 0/3</td>
<td>1</td>
<td>Used</td>
<td>access</td>
<td>ADBEDC01</td>
</tr>
<tr>
<td>fa 0/4</td>
<td>-</td>
<td>Not Used</td>
<td>-</td>
<td></td>
</tr>
<tr>
<td>fa 0/5</td>
<td>-</td>
<td>Not Used</td>
<td>-</td>
<td></td>
</tr>
<tr>
<td>fa 0/6</td>
<td>-</td>
<td>Not Used</td>
<td>-</td>
<td></td>
</tr>
<tr>
<td>fa 0/7</td>
<td>-</td>
<td>Not Used</td>
<td>-</td>
<td></td>
</tr>
<tr>
<td>fa 0/8</td>
<td>-</td>
<td>Not Used</td>
<td>-</td>
<td></td>
</tr>
<tr>
<td>fa 0/9</td>
<td>20</td>
<td>Used</td>
<td>access</td>
<td>Wireless client</td>
</tr>
<tr>
<td>fa 0/10</td>
<td>-</td>
<td>Not Used</td>
<td>-</td>
<td></td>
</tr>
<tr>
<td>fa 0/11</td>
<td>-</td>
<td>Not Used</td>
<td>-</td>
<td></td>
</tr>
<tr>
<td>fa 0/12</td>
<td>-</td>
<td>Not Used</td>
<td>-</td>
<td></td>
</tr>
<tr>
<td>fa 0/13</td>
<td>30</td>
<td>Used</td>
<td>access</td>
<td>Wireless client</td>
</tr>
</tbody>
</table>

**Configuring VLANs on the switch**

First, you need to configure the required VLANs on your switch. You configure them from Global Configuration mode.

ADDEVSW# config t
ADDEVSW(config)# vlan 20
ADDEVSW(config-vlan)# name wireless_network_scooby_doo
Configuring wireless dynamic VLANs on Windows Server 2008, version 1.0

Viewing VLAN configuration:

ADDEVSW#  sh vlan

Assigning Switch Ports to VLANs

The next step is to assign the switch ports to the appropriate VLAN. A switch port can only be a member of one VLAN at the time.

ADDEVSW#  config t
ADDEVSW(config)#  int fa0/3
ADDEVSW(config-if)#  switchport access vlan 1
ADDEVSW(config-if)#  int fa0/9
ADDEVSW(config-if)#  switchport access vlan 20
ADDEVSW(config-if)#  int fa0/13
ADDEVSW(config-if)#  switchport access vlan 30
ADDEVSW(config-if)#  end

Viewing VLAN configuration:

ADDEVSW#  sh vlan
Configuring Trunk Ports

The next step is to configure the required ports as trunks, to forward traffic to all user-defined VLANs.

```
ADDEVSW# config t
ADDEVSW(config)# int fa0/1
ADDEVSW(config-if)# switchport mode trunk
ADDEVSW(config-if)# switchport trunk native vlan 1
ADDEVSW(config-if)# switchport nonegotiate
ADDEVSW(config-if)# int fa0/2
ADDEVSW(config-if)# switchport mode trunk
ADDEVSW(config-if)# switchport trunk native vlan 1
ADDEVSW(config-if)# switchport trunk nonegotiate
ADDEVSW(config-if)# switchport trunk allowed vlan add 1,20,30
ADDEVSW(config-if)# end
```

Viewing trunk configuration:

```
ADDEVSW# sh int fa0/1 trunk
```

Viewing VLAN configuration:

```
ADDEVSW# sh int fa0/1 trunk
```
Configure Cisco Router 2621

Only hosts that are connected to the same VLAN can communicate. To allow communication between the VLANs, you need a layer three switch or a router.

In order to support trunking and inter-VLAN routing, the router must have a FastEthernet interface. To connect all VLANs together to allow inter-VLAN communication, we use a router on a stick. This because we use only a router with one interface that we need to configure with 802.1Q trunking.

The next step is to create an 802.1Q trunk between the router and the switch/access point to allow communication between the different VLANs.

The interface of the router is divided into subinterfaces, this to support all the VLANs we need.

- Configure the router to support inter-VLAN routing

Configure the router to support inter-VLAN routing

```
ADDEVTRTR# config t
ADDEVTRTR(config)# int fa0/0
ADDEVTRTR(config-if)# no ip address
ADDEVTRTR(config-if)# no shutdown
ADDEVTRTR(config-if)# int fa0/0.1
ADDEVTRTR(config-subif)# encapsulation dot1q 1
```
Configure the wireless access point

The wireless access point supports multiple SSIDs that can be associated with VLANs. This gives use the opportunity to use different security models for different SSIDs.

In this design we use two types of authentication/encryption methods. You need to configure the wireless access point with two SSIDs:

SSID1: SCOOBYDOO, use Open Authentication in combination with WPA-Enterprise and TKIP. When the user connects to this wireless network, the user sends his certificate to the NPS server for authentication. Encryption is done through WPA on the NPS Server.

SSID2: TWINPEAKS, use Open Authentication (802.1x) and Dynamic WEP Encryption. When the user connects to the wireless network, authentication is done through EAP and use dynamic WEP encryption performed by the NPS server.

The wireless access point is by default configured to receive an IP address from a DHCP Server.

- Configure the wireless interface Radio0 with a static IP address
- Configure IP Settings on the wireless access point
- Enable the Radio Interface
- Define the first wireless network
- Define the second wireless network
- Configure Encryption Mode for VLAN 20
- Configure Encryption Mode for VLAN 30
- Configure Authentication Method for SCOOBYDOO wireless network
• Configure Authentication Method for TWINPEAKS wireless network
• Define RADIUS Authentication on the wireless access point
• Define RADIUS Server Priorities

**Configure the wireless interface Radio0 with a static IP address**

```plaintext
AP# config t
AP(config)# int BVI1
AP(config-if)# no ip address dhcp
AP(config-if)# ip address 172.16.10.230 255.255.255.0
AP(config-if)# end
```

**Configure IP Settings on the wireless access point**

♦ From a computer on VLAN 1, open *Internet Explorer* and type http://172.16.10.230 in the address bar.

♦ Select *Express Set-up*, specify the required settings and click *Apply*.

![Image of Cisco Aironet 1130AG Series Access Point](image)

**Enable the Radio0 Interface**

♦ Click on *Network Interfaces*, click on *Radio0-208.11G*, click on the *Settings* tab, and select *Enable Radio*. Click *Apply*.
Define the first wireless network

- Click on Express Security. In this section you can specify your SSID Configuration:
  - 1. SSID: type SCOOBYDOO
  - 2. VLAN: select Enable VLAN ID and type 20
  - 3. Security: select WPA. Under RADIUS Server type the IP address of your internal NPS Server, which is 172.16.10.3. Under RADIUS Server Secret type the RADIUS secret, which must be same value as you typed on the NPS server. Click Apply
Define the second wireless network

- Click on **Express Security**. In this section you can specify your SSID Configuration:
  1. SSID: type TWINPEAKS
  2. VLAN: select Enable VLAN ID and type 30
  3. Security: select WPA. Under RADIUS Server type the IP address of your internal NPS Server, which is 172.16.10.3. Under **RADIUS Server Secret** type the RADIUS secret, which must be same value as you typed on the NPS server. Click **Apply**

Configure Encryption Mode for VLAN 20

- Click on **Security**. Select **Encryption Manager**. On **Set Encryption Mode and Keys for VLAN**, select 20 from the list box.
- Under **Encryption Modes**, select **Cipher** and select **TKIP** from the list box.
- Click **Apply**
Configure Encryption Mode for VLAN 30

- Click on Security. Select Encryption Manager. On Set Encryption Mode and Keys for VLAN, select 30 from the list box.
- Under Encryption Modes, select WEP Encryption and select Mandatory from the list box.
- Click Apply

Configure Authentication Method for SCOOBYDOO wireless network

- Click on SSID Manager. From the Current SSID list, select SCOOBYDOO
Under **Client Authentication Settings**, select **Open Authentication** and select with EAP from the list box. Also select **Network EAP** and select **<NO ADDITION>** from the list box.

Under **Client Authenticated Key Management**, select **Mandatory** and select **WPA**.

Click **Apply**.

**Configure Authentication Method for TWINPEAKS wireless network**

- Click on **SSID Manager**. From the Current SSID list, select TWINPEAKS
- Under **Client Authentication Settings**, select **Open Authentication** and select with EAP from the list box. Ensure that **Network EAP** is not enabled.
- Under **Client Authenticated Key Management**, select **<NONE>**
- Click **Apply**.
Define RADIUS Authentication on the wireless access point

- Click on Server Manager.
- From the current server list, select the IP address of your NPS server.
- Change the value after Authentication Port to 1812
- Change the value after Accounting Port to 1813
- Click Apply
Define RADIUS Server Priorities

- From **Default server priorities**, select the following:
  - EAP Authentication: select the IP address of your NPS server from the list box
  - Accounting: select the IP address of your NPS server from the list box
  - Admin Authentication: select the IP address of your NPS server from the list box
- Click **Apply**
Configure Client Computer for wireless access

In this section you need to configure the client computers with wireless networks and assumes that the client computers and user accounts already have a certificate and that the client computer is a member of the domain.

You can also configure the wireless networks via a group policy.

- Create a wireless network connection for SCOOBYDOO wireless network
- Configure Authentication Methods for SCOOBYDOO wireless network
- Connect to SCOOBYDOO wireless network
- Verify wireless client computer IP address settings
- Create a wireless network connection for TWINPEAKS wireless network
- Configure Authentication Methods for TWINPEAKS wireless network
- Connect to TWINPEAKS wireless network
- Verify wireless client computer IP address settings

Create a wireless network connection for SCOOBYDOO wireless network

- Open Network and Sharing Center, select Set up a connection or network.
- On the Choose a connection option page, select Manually connect to a wireless network and click Next.

Configuring wireless dynamic VLANs on Windows Server 2008, version 1.0
On the **Enter Information for the wireless network you want to add** page, specify the requested information, for example:
- Network name: SCOOBYDOO
- Security type: WPA-Enterprise
- Encryption type: TKIP

Select **Connect even if the network is not broadcasting** and clear **Start this connection automatically**. Click **Next**.
• Click Close

Configure Authentication Methods for SCOOBYDOO wireless network

• Right click on SCOOBYDOO wireless network and select Properties

• Click on the Security tab, from Choose a network authentication method, select Smart card or certificate and click OK
Connect to SCOOPYDOO wireless network

- Select **Connect to a network**, right click on SCOOPYDOO and select **Connect**.
- After successfully authentication, you are connected to the wireless network.
Verify wireless client computer IP address settings

- Open **command prompt** and type `ipconfig`

Create a wireless network connection for TWINPEAKS wireless network

- Open **Network and Sharing Center**, select **Set up a connection or network**.
- On the **Choose a connection option** page, select **Manually connect to a wireless network** and click **Next**.
On the **Enter Information for the wireless network you want to add** page, specify the requested information, for example:
- Network name: TWINPEAKS
- Security type: 802.1x
- Encryption type: WEP

Select **Connect even if the network is not broadcasting** and clear **Start this connection automatically**. Click **Next**.

Click **Close**
Configure Authentication Methods for TWINPEAKS wireless network

- Right click on TWINPEAKS wireless network and select **Properties**

- Click on the **Security** tab, from **Choose a network authentication method**, select **Smart card or certificate** and click **OK**
Connect to TWINPEAKS wireless network

- Select **Connect to a network**, right click on TWINPEAKS and select **Connect**.
- After successfully authentication, you are connected to the wireless network.
Verify wireless client computer IP address settings

- Open **command prompt** and type **ipconfig**

![Command Prompt Output](image)
## Appendix A: Overview of security groups

<table>
<thead>
<tr>
<th>Security group</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Wireless Users VLAN 20</td>
<td>Global group for users who require access to VLAN 20</td>
</tr>
<tr>
<td>Wireless Users VLAN 30</td>
<td>Global group for users who require access to VLAN 30</td>
</tr>
<tr>
<td>AutoEnroll NPS Server Authentication Certificate</td>
<td>Global group for NPS server computer accounts</td>
</tr>
<tr>
<td>AutoEnroll Client Authentication – Computer Certificate</td>
<td>Global group for computers that require a computer certificate</td>
</tr>
</tbody>
</table>
Appendix B: Log Results for SCOOPYDOO Wireless Network

<table>
<thead>
<tr>
<th>Name</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Computer-Name</td>
<td>ADHLSRV01</td>
</tr>
<tr>
<td>Service-Name</td>
<td>IAS</td>
</tr>
<tr>
<td>Record-Date</td>
<td>08/10/2007</td>
</tr>
<tr>
<td>Record-Time</td>
<td>12:49:01</td>
</tr>
<tr>
<td>Packet-Type</td>
<td>Access-Request</td>
</tr>
<tr>
<td>User-Name</td>
<td><a href="mailto:stef@addex.local">stef@addex.local</a></td>
</tr>
<tr>
<td>Fully-Qualified-User-Name</td>
<td>addex.local/Access Denied/Users/Stef Looe</td>
</tr>
<tr>
<td>Called Station-Id</td>
<td>0018 7443 3430</td>
</tr>
<tr>
<td>Calling-Station-Id</td>
<td>0019 963e 4527</td>
</tr>
<tr>
<td>NAS-Identifier</td>
<td>ap</td>
</tr>
<tr>
<td>NAS-IP-Address</td>
<td>172.16.10.230</td>
</tr>
<tr>
<td>NAS-Port</td>
<td>257</td>
</tr>
<tr>
<td>Client-Vendor</td>
<td>RADIUS Standard</td>
</tr>
<tr>
<td>Client-IP-Address</td>
<td>172.16.10.230</td>
</tr>
<tr>
<td>Client-Friendly-Name</td>
<td>Cisco 1130 AP</td>
</tr>
<tr>
<td>Port-Limit</td>
<td>0</td>
</tr>
<tr>
<td>NAS-Port-Type</td>
<td>Wireless - IEEE 802.11</td>
</tr>
<tr>
<td>Framed-Protocol</td>
<td>0</td>
</tr>
<tr>
<td>Service-Type</td>
<td>Login</td>
</tr>
<tr>
<td>Authentication-Type</td>
<td>EAP</td>
</tr>
<tr>
<td>NP-Policy-Name</td>
<td>Wireless Users - VLAN 20</td>
</tr>
<tr>
<td>Reason-Code</td>
<td>IAS_SUCCESS</td>
</tr>
<tr>
<td>Class</td>
<td>3171 1 08/10/2007 10:46:13 5</td>
</tr>
<tr>
<td>Session-Timeout</td>
<td>0</td>
</tr>
<tr>
<td>Idle-Timeout</td>
<td>0</td>
</tr>
<tr>
<td>Termination-Action</td>
<td>Default</td>
</tr>
<tr>
<td>EAP-Friendly-Name</td>
<td>Microsoft: Smart Card or other certificate</td>
</tr>
<tr>
<td>Acct-Status-Type</td>
<td>0</td>
</tr>
<tr>
<td>Acct-Delay-Time</td>
<td>0</td>
</tr>
<tr>
<td>Acct-Input-Packets</td>
<td>0</td>
</tr>
<tr>
<td>Acct-Input-Bytes</td>
<td>0</td>
</tr>
<tr>
<td>Acct-Link-Count</td>
<td>0</td>
</tr>
<tr>
<td>Acct-Interval</td>
<td>0</td>
</tr>
<tr>
<td>Tunnel-Type</td>
<td>0</td>
</tr>
<tr>
<td>Tunnel-Medium-Type</td>
<td>0</td>
</tr>
<tr>
<td>Tunnel-Preference</td>
<td>0</td>
</tr>
<tr>
<td>MS-Acct-Auth-Type</td>
<td>0</td>
</tr>
<tr>
<td>MS-Acct-EAP-Type</td>
<td>0</td>
</tr>
<tr>
<td>MS-RAS-Vendor</td>
<td>RADIUS Standard</td>
</tr>
<tr>
<td>MS-MPPE-Encryption-Types</td>
<td>0</td>
</tr>
<tr>
<td>MS-MPPE-Encryption-Policy</td>
<td>0</td>
</tr>
<tr>
<td>Proxy-Policy-Name</td>
<td>Secure Wireless Access</td>
</tr>
<tr>
<td>Provider-Type</td>
<td>Windows</td>
</tr>
</tbody>
</table>

Number of links in a multi-link session
### Appendix C: Log results for TWINPEAKS Wireless Network

<table>
<thead>
<tr>
<th>Name</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Computer Name</td>
<td>ADLHsrv01</td>
</tr>
<tr>
<td>Service Name</td>
<td>IAS</td>
</tr>
<tr>
<td>Record Time</td>
<td>08/10/2007</td>
</tr>
<tr>
<td>Packet-Request</td>
<td>Access-Request</td>
</tr>
<tr>
<td>Username</td>
<td><a href="mailto:johan@addex.local">johan@addex.local</a></td>
</tr>
<tr>
<td>Fully-Qualified-User-Name</td>
<td>addex.local/Access Denied/Users/Johan Loss</td>
</tr>
<tr>
<td>Called-Station-Id</td>
<td>0018 74d3 3d30</td>
</tr>
<tr>
<td>Calling-Station-Id</td>
<td>0019 7d0e 4527</td>
</tr>
<tr>
<td>NAS-Identifier</td>
<td>ap</td>
</tr>
<tr>
<td>NAS-IP-Address</td>
<td>172.16.10.230</td>
</tr>
<tr>
<td>NAS-Port</td>
<td>273</td>
</tr>
<tr>
<td>Client-Vendor</td>
<td>RADIUS Standard</td>
</tr>
<tr>
<td>Client-IP-Address</td>
<td>172.16.10.230</td>
</tr>
<tr>
<td>Client-Friendly-Name</td>
<td>Cisco 1130 AP</td>
</tr>
<tr>
<td>Port-Limit</td>
<td>0</td>
</tr>
<tr>
<td>NAS-Port-Type</td>
<td>Wireless - IEEE 802.11</td>
</tr>
<tr>
<td>Framed-Protocol</td>
<td>0</td>
</tr>
<tr>
<td>Service-Type</td>
<td>Login</td>
</tr>
<tr>
<td>Authentication-Type</td>
<td>EAP</td>
</tr>
<tr>
<td>NP-Profile-Name</td>
<td>Wireless Users - VLAN 30</td>
</tr>
<tr>
<td>Reason-Code</td>
<td>IAS_SUCCESS</td>
</tr>
<tr>
<td>Class</td>
<td>31111 108/10/2007 10:46:19.28</td>
</tr>
<tr>
<td>Session-Timeout</td>
<td>0</td>
</tr>
<tr>
<td>Idle-Timeout</td>
<td>0</td>
</tr>
<tr>
<td>Termination-Action</td>
<td>Default</td>
</tr>
<tr>
<td>EAP-Friendly-Name</td>
<td>Microsoft: Smart Card or other certificate</td>
</tr>
<tr>
<td>Acct-Status-Index</td>
<td>0</td>
</tr>
<tr>
<td>Acct-Delay-Time</td>
<td>0</td>
</tr>
<tr>
<td>Acct-Input-Octets</td>
<td>0</td>
</tr>
<tr>
<td>Acct-Output-Octets</td>
<td>0</td>
</tr>
<tr>
<td>Acct-Authentic</td>
<td>None</td>
</tr>
<tr>
<td>Acct-Session-Change</td>
<td>0</td>
</tr>
<tr>
<td>Acct-Input-Packets</td>
<td>0</td>
</tr>
<tr>
<td>Acct-Output-Packets</td>
<td>0</td>
</tr>
<tr>
<td>Acct-Terminate-Cause</td>
<td>0</td>
</tr>
<tr>
<td>Acct-LINK-COUNT</td>
<td>0</td>
</tr>
<tr>
<td>Acct-INTER-Interval</td>
<td>0</td>
</tr>
<tr>
<td>Tunnel-Type</td>
<td>0</td>
</tr>
<tr>
<td>Tunnel-Medium-Type</td>
<td>0</td>
</tr>
<tr>
<td>Tunnel-Preference</td>
<td>0</td>
</tr>
<tr>
<td>MS-Acct-Auth-Type</td>
<td>0</td>
</tr>
<tr>
<td>MS-Acct-Message-Type</td>
<td>0</td>
</tr>
<tr>
<td>MS-RAS-Vendor</td>
<td>RADIUS Standard</td>
</tr>
<tr>
<td>MS-MPPE-Esperations-Types</td>
<td>0</td>
</tr>
<tr>
<td>MS-MPPE-Esperations-Policy</td>
<td>0</td>
</tr>
<tr>
<td>Proxy-Policy-Name</td>
<td>Secure Wireless Access</td>
</tr>
<tr>
<td>Provider-Type</td>
<td>Windows</td>
</tr>
</tbody>
</table>