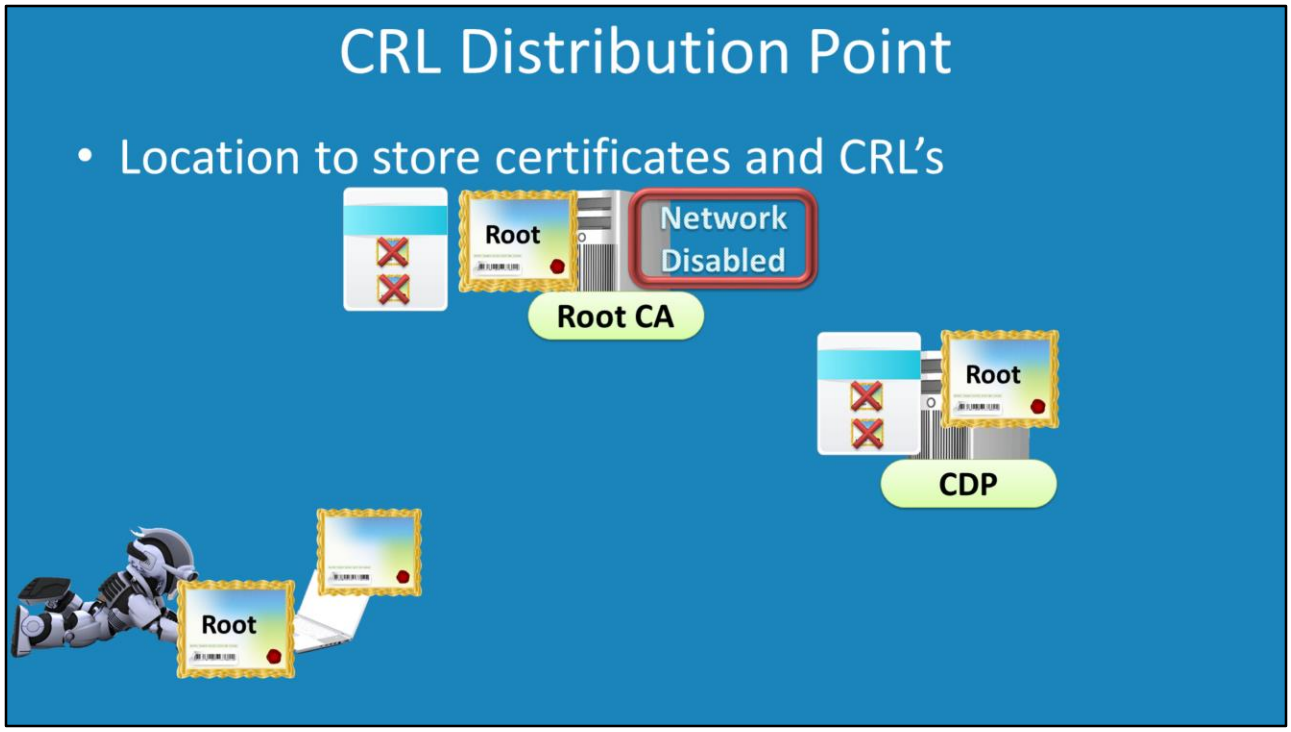
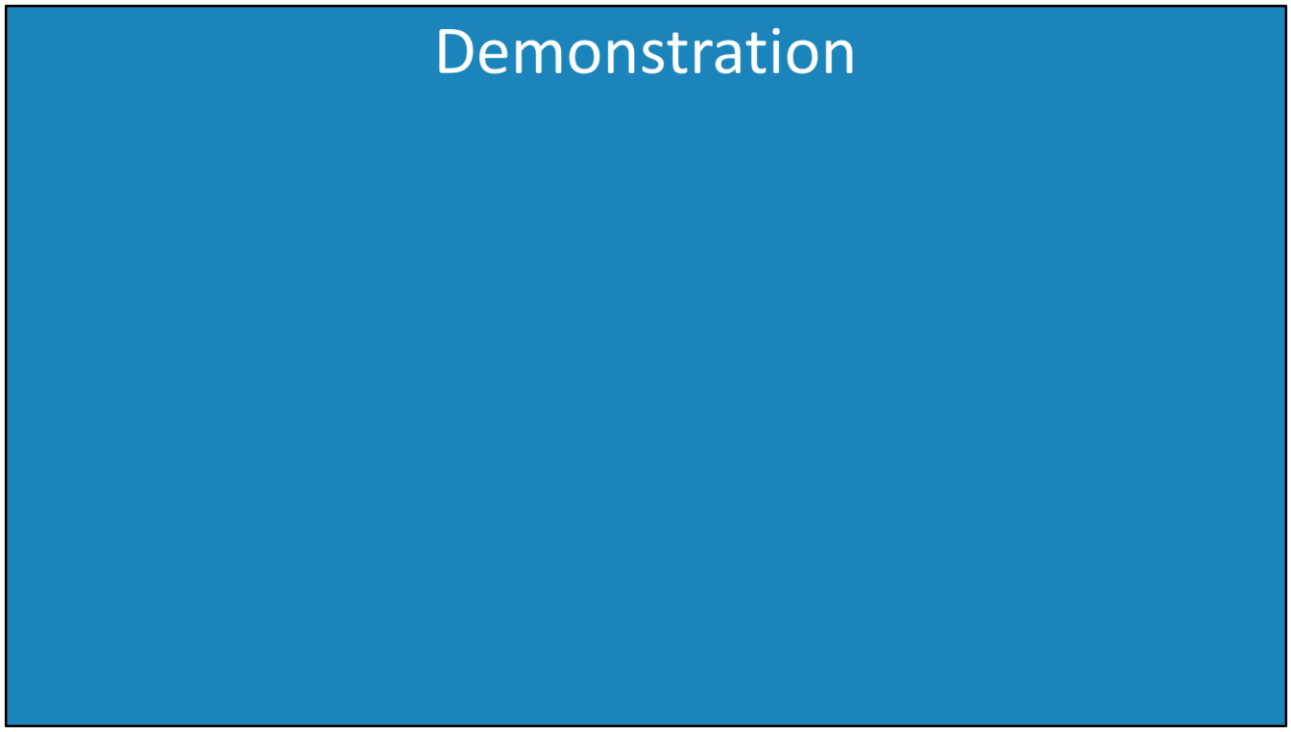
Before a certificate can be used it is a best practice to check the certificate to ensure that it has not been revoked. In order to do this, the list called the Certificate Revocation Lists (CRL) needs to be stored on the network so that clients can access it and also be updated when certificates are revoked.



CRL Distribution Points

To put it in simple terms, a CRL distribution point is a shared location on the network that is used to store the CRL and certificates. A CRL contains all the certificates on the network that have been revoked. A client needs to download this list to determine if the certificate that they are about to use is valid. Certificates are required to be stored in the distribution point to make it simple for clients to obtain them. When a certificate is verified, the root CA and other subordinate CA's are required in order to verify each part of the certificate chain. A distribution point provides a point on the network for clients to download these certificates, otherwise the certificates would have to be manually installed on the client's computer.

A CDP stands for CRL Distribution Point. This can be accessible by web, LDAP or file share. The location of the CDP is stored in the certificate so when the client obtains a certificate it knows to look inside the certificate to obtain this information.



Demonstration
This demonstration will create a distribution point that is available via www, files share and LDAP.

Open server manager, select roles and then select the option add roles.
From the roles screen, select the role Web Server (IIS). No other components are required, so accept all the defaults and complete the wizard.
In order to have somewhere to save the files, create a folder on the c drive called CertEntroll
To allow clients to access this folder by file sharing, right click the folder and select properties. Then select the sharing tab and then press the button advanced sharing.
In the advanced sharing, make sure the tick box “Share this folder is ticked”.
The default permissions are read only which will be enough for clients to access. In order to update the CRL additional permissions are required. In order to configure these, press the button permissions and then add the group Cert Publishers with change access so that this group can write to that folder.
The NTFS permissions also need to be changed. To do this, select the security tab and then press the button edit. In here you need to add the group Cert Publishers. In order to grant write access, make sure the permission modify and below are ticked.
To configure the directory to be available via a web page, this needs to be configured in IIS. To do this, open Internet information Services (IIS) Manager from administrative tools under the start menu.

From IIS, expand down through until you reach Default Web Site. Right click Default Web Site and select the option Add Virtual Directory. For alias enter in CertEnroll and then browse to the directory c:\CertEnroll. When clients access the web server on this server, the C:\CertEntroll directory will appear under
http://servername/CertEnroll
By default IIS will not display the contents of a directory and thus requires the user to know which file in the folder they want to access. To change this, under the virtual directory CertEnroll, select the option Directory Browsing. Once selected, on the far right is an option enable which needs to be selected in order to allow directory browsing.
The last option that is required to be configured in IIS is to allow double escaping. This is required by the CRL in order to work. The following file contains a script that enables double escaping
http://itfreetraining.com/handouts/certificates/cadownloadfiles.zip. In this file is the script ConfigureWebServer.bat which you need to run. Otherwise you run the commands listed below.

```
cd %windir%\System32\inetsrv
C:\Windows\System32\inetsrv\Appcmd set config "Default Web Site"
/section:system.webServer/Security/requestFiltering -allowDoubleEscaping:True
Iisreset
```

Once the command is run. IIS needs to be restarted. This can be done manually or using the command IISReset like what has been done above.
In this case, I will copy the root CA and CRL from the root CA to the distribution point. In order to do this, login to the root CA and then access the directory C:\Windows\System32\CertSrv\CertEnroll
In this directory is the certificate for the root CA and the CRL for the root CA. In a previous video the root CA was set up, however the root CA was configured never to publish updates to the CRL. Even though the root CA will never publish updates, the base CRL list still needs to be copied from here to the distribution point so clients can check the root CA has not revoked any certificates.
The two files from the root ca C:\Windows\System32\CertSrv\CertEnroll need to be copied to the directory c:\CertEnroll on the server that has the CDP on it.
The certificate and CRL needs to also be published in Active Directory in order for clients in the domain to be able to use LDAP to locate these files. There is a script in the following download
http://itfreetraining.com/handouts/certificates/cadownloadfiles.zip called AddCertAndCRLToAD.bat
This file contains the following two commands.

```
CertUtil -f -DSPublish RootCA_ITFreeTraining-Root-CA.crt RootCA
CertUtil -f -DSPublish ITFreeTraining-Root-CA.crl RootCA
```

–f stands for to take information from a file. DSPublish means store in Active

Directory. The next parameter indicates the file that is to be stored in active directory, either the certificate or the CRL file. The first command ends with RootCA which tells Active Directory that the certificate is for a Root CA. You could also use SubCA, user or machine depending on which type of certificate you are publishing in Active Directory.
In the case of the second command it also ends with RootCA like the first. However, this is the computer name of the RootCA. In this example, the root CA I have used has the computer name of RootCA. If your RootCA has a different computer name you will need to change this to the name of the RootCA>

Seeing the data in Active Directory
Open ADSI Edit from the start menu. Right click ADSI at the top and select the option Connect to. Under the option "Select a well known naming context" select the option Configuration.
Expand down through Configuration, Services, Public Key Services and AIA. In this container you should see the certificate for the root CA.
Expand down through Configuration, Services, Public Key Services, CDP and Root CA. This should contain the CRL.

Configuring the DNS Server
In this case the domain has a DNS address of .local. If you want to have the distribution point available on the internet, you will need to use an address that is resolvable from the internet. In this case I will create a new zone called ITFreeTraining.com to store a DNS record that will be used to direct a user from the internet to the server in the .local domain. If you do this, you need to ensure that this server is accessible for the internet in order for this to work.

To create a new zone, right click on Forward Look up zone and then finish the wizard. For the zone enter in the name ITFreeTraining.com
Select the newly created zone and then select from the action menu the option New Alias (CName).
Create a DNS record called PKI and link it to the server that you are using as a distribution point.

See http://YouTube.com/ITFreeTraining or http://itfreetraining.com for our always free training videos. This is only one video from the many free courses available on YouTube.

References
"AD CS Step by Step Guide: Two Tier PKI Hierarchy Deployment"
http://social.technet.microsoft.com/wiki/contents/articles/15037.ad-cs-step-by-step-guide-two-tier-pki-hierarchy-deployment.aspx