

1. Overview

802.1x is a method for port-based network access control (NAC). It provides authentication for devices plugged into a LAN port or connected to a wireless access point.

Currently, SCHOOLNAME School only uses it for wireless authentication but there are plans to enable it for all hard-wired devices too.

To explain further; in a wireless network with 802.1X, a user or computer (referred to as the supplicant) requests access to an access point (the authenticator). The access point forces the user or computer into an unauthorized state that allows the client to send only an EAP start message. The access point returns an EAP message requesting the user's or computer's identity. The supplicant returns the identity, which is then forwarded by the access point to the authentication server (RADIUS), which uses policies and other checks (i.e. checking if the user and/or computer exists in the database i.e. Active Directory), to authenticate the user or computer and then returns an accept or reject message back to the access point. Assuming an accept was received, the access point changes the client's state to authorized and it can now communicate on the network.

2. Configuration

RADIUS authentication services are provided by Network Policy Server which is an installed "feature" on SCHOOLNAME-DC3, a virtual server running Windows Server 2008 R2.

A backup installation of NPS is on SCHOOLNAME-DC2 to provide redundancy.

This outlines the steps required to setup NPS to provide RADIUS or 802.1x authentication:

2.2 Obtaining an SSL certificate

In order for us to be able to use RADIUS PEAP authentication a certificate is required so that the supplicant (laptop client) can verify the identity of the RADIUS server before connecting.

The certificate used by SCHOOLNAME-DC3 was obtained from SCHOOLNAME-DC1, the domain's certification authority server – and this is how:

1. Click Start --> Run and type MMC to open management console.
2. Click File > Add/Remove Snap In
3. On the drop down menu select Console Root and then click Add.
4. Select the Certificates snap in and then click Add.
5. Click Computer Account > Next make sure Local Computer is selected.
6. Expand the Certificate (Local Computer) and click on Personal store
7. Right click on Certificates and select All Tasks --> Request New Certificate.
8. Make sure Server or Computer is selected and then click Next.
9. Give a friendly name to the certificate and also provide a description for what the certificate is going to be used for and click Next
10. The final box will give you a summary of the details entered and issue a certificate.

NB: The issuing certificate authority (in this case, SCHOOLNAME-dc1, is set as a trusted authority in Group Policy – this is configured under the wireless 802.1x security policy in a GPO).

2.3 Configuring NPS

These are the steps for configuring NPS to authenticate wireless users:

1. Open NPS
2. On the Getting Started screen choose "RADIUS server for 802.1x Wireless or Wired Connections" and then click "Configure 802.1x"
3. Select "Secure Wireless Connections" and give the policy a suitable name.
4. You will now be asked to enter the details of any RADIUS clients (authenticators). Click add and type in the name and IP address of the Ruckus ZoneDirector, and manually specify a shared secret (widget) (make sure that you write this down somewhere safe as you will need to use it when you configure the ZoneDirector to talk to a RADIUS server!).
5. You will now be prompted for an authentication method. Select "Microsoft: Protected EAP (PEAP)" and click the Configure button.
6. Ensure that the certificate you created in step 2.2 is selected and that "Enable Fast Reconnect" is ticked. Click OK and then Next.
7. You are now asked to confirm which groups will be used with this policy to enable access. Click Add, change the location box to "SCHOOLNAME.co.uk" and select "Domain Computers". Click Next
8. On the next screen you are asked to "Configure Traffic Controls" – this allows you to put traffic into certain VLANs or apply ACLs. We are not currently using this so click Next.
9. Click Finish!

That's it.

NB: A backup of the NPS configuration is stored on SCHOOLNAME-NAS6.