How To | Configure A Secure Network Solution For Schools

Introduction

This How To Note describes a secure network solution configuration for schools. In the configuration there are two network segments (VLANs): admin and curriculum. The admin VLAN is protected by a stateful inspection firewall to prevent students accessing records etc. Teachers, connecting in classroom areas, need to connect to any available socket and see the curriculum material. In addition, they need access to the admin network to check records etc. This access is username/password protected so that pupils cannot access the admin areas. PPP over Ethernet (PPPoE) is used to provide this access for teachers.

Of course, this application can be used in any environment where there are secure and public sections of the LAN and users connected to the public area who need access to parts of the secure area.

What information will you find in this document?

This Note provides:

- a secure network solution for schools in step-by-step format, starting on page 3.
- the script-only version of the solution on page 10.

Which products does it apply to?

This Note applies to the following Allied Telesis managed layer 3 switches, running software version 2.6.4 or later:

- AT-8800, Rapier, and Rapier i series switches
- AT-9800 series switches

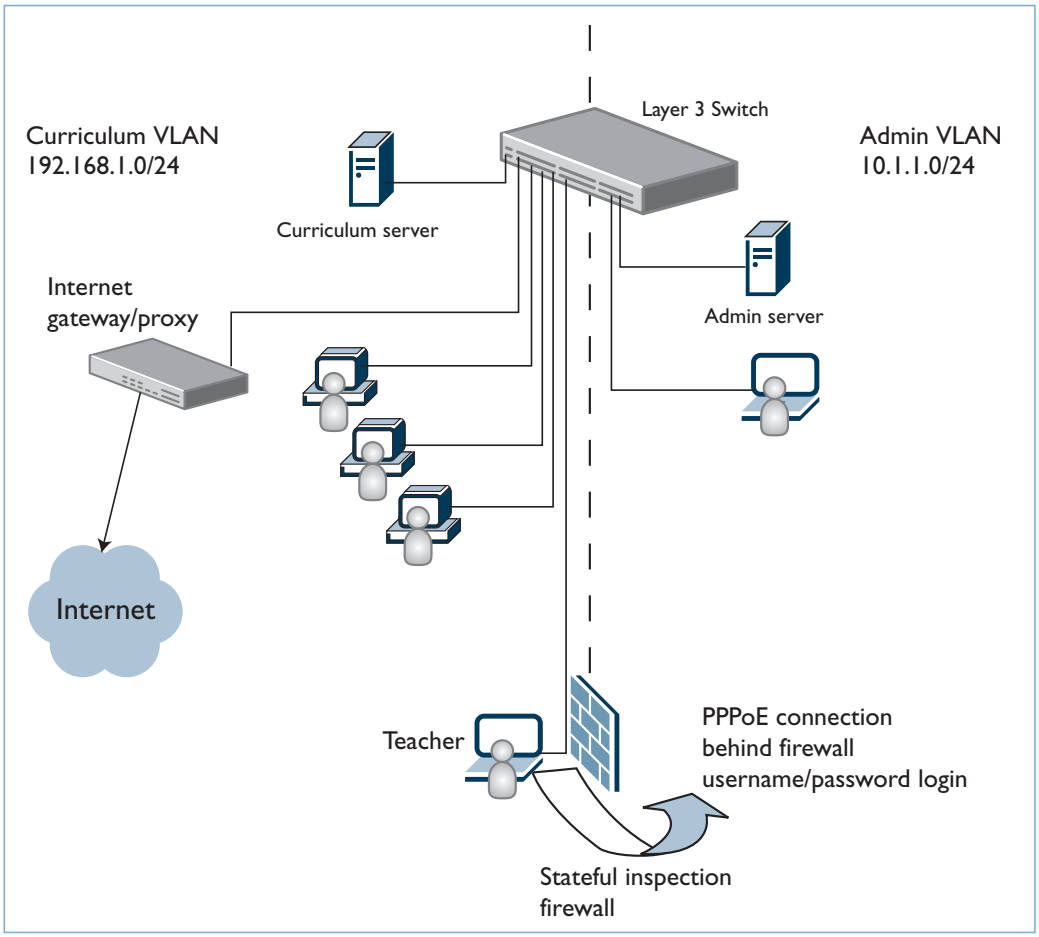
Related How To Notes

You also may find the following How To Notes useful:

- *How To Apply Firewall Policies And Rules*
- *How To Allow Public And Private Address Access To Servers At A Service Provider Client Site*
- *How To Configure A Secure School Network Based On 802.1x*

How To Notes are available from www.alliedtelesis.com/resources/literature/howto.aspx.

Description of the configuration



In the network configuration illustrated above, the switch has two VLANs: curriculum and admin. Ports on the admin VLAN are located in secure areas in the school where pupils do not have access, such as the staff room, offices etc. All ports that are openly available are assigned to the curriculum VLAN. Each VLAN is assigned an IP address, 192.168.1.1 for the curriculum VLAN and 10.1.1.1 for the admin VLAN. The firewall is enabled on the switch, with the curriculum VLAN on the public side and admin VLAN on the private side. This allows users on the admin VLAN to open sessions to servers on the curriculum VLAN, but prevents pupils on the curriculum VLAN from accessing any secure servers in the admin VLAN.

How can teachers log into the admin LAN from the classroom?

The switch is configured to be a PPPoE Access Server. When a teacher starts their PPPoE client (using WinPoet or similar) they will get a login/password prompt. The switch will authenticate the teacher against its user database or against a RADIUS server database if there are a lot of teachers. The teacher is assigned an IP address, and a PPP link is created to the switch. This new PPP link is then dynamically added to the firewall as a private interface, allowing the teachers to see the admin servers and resources. The PPP link times out after 10 minutes, or if the teacher's PC is disconnected from the Ethernet connection, ensuring that the network remains secure.

The switch can also act as a DHCP server to assign IP addresses in the appropriate range for the admin and curriculum VLANs. This makes it easier for teachers to connect to either segment.

Internet access is possible via an Internet gateway router or firewall/proxy server. Many schools use a proxy to ensure that there is no inappropriate use of the Internet. In this configuration, the device only needs an interface to the curriculum network since the firewall can be configured to do NAT (Network Address Translation) between the admin network and its address on the curriculum network. This means that there is no additional configuration required on the gateway to account for the two networks that are connected.

Configuration of the switch

Before you start, check you have the firewall feature licence activated, by using the command:

```
show feature
```

Note: If you do not have a firewall licence, contact your nearest Allied Telesis representative to purchase one.

1. Set the system name

Set the system name, which helps to remind you which switch you have logged into!

```
set system name=school.firewall
```

2. Configure the VLANs

Create the admin VLAN. For this example we are using the default VLAN for curriculum use.

```
create vlan=admin vid=2
add vlan=2 port=17-24
```

3. Configure IP

Set the IP parameters, and add the two VLAN IP addresses.

```
enable ip
add ip interface=vlan1 ip=192.168.1.1 mask=255.255.255.0
add ip interface=vlan2 ip=10.1.1.1 mask=255.255.255.0
```

Then add a default route to the internet gateway

```
add ip route=0.0.0.0 mask=0.0.0.0 interface=vlan1 next=192.168.1.254
```

You should now have open access between the 10.1.1.0 subnet and the 192.168.1.0 subnet. You can test this using two PCs.

4. Configure the firewall

The next step is to set up the firewall.

Initially, create a policy called 'a' and assign the curriculum and admin VLANs as public and private interfaces. Then set up NAT between the addresses on the admin VLAN and the curriculum interface. The configuration is as follows:

```
enable firewall
create firewall policy=a
add firewall policy=a interface=vlan2 type=private
add firewall policy=a interface=vlan1 type=public
add firewall policy=a nat=enhanced interface=vlan2 gblinterface=vlan1
```

You should now have the ability to use the existing Internet gateway router or firewall, to access the Internet. You need to put static addresses on your PCs to test this. Remember to set the gateway address correctly. The gateway IP address for PCs in the curriculum VLAN is 192.168.1.1, and 10.1.1.1 for PCs in the admin VLAN.

This is now a configuration that allows the admin VLAN to be protected and only accessed when the teachers connect to a port in that VLAN. Since we don't want to put admin ports in the classrooms we will set up PPPoE (after configuring the switch as a DHCP server).

Configuring the switch as a DHCP server

The switch can act as a DHCP server, which makes the correct IP assignment easier and allows teachers to move between the admin and curriculum areas. This is optional. You may instead choose to use a separate DHCP server for the curriculum and admin VLANs.

In the following configuration, we set the default gateway address for each VLAN to the IP address on the switch. The DNS address (DNSS) is set to the address for the gateway router (or firewall if you are using one). If you are using a proxy server for Internet access and content filtering, then the DNSS line is not required. Further details of other DHCP settings can be found in your software reference.

1. Enable the DHCP server

```
enable dhcp
```

2. Configure a DHCP policy for the curriculum VLAN

```
create dhcp policy=base1 leasetime=7200
add dhcp policy=base1 subnet=255.255.255.0
add dhcp policy=base router=192.168.1.1
add dhcp policy=base dnsserver=192.168.1.254
create dhcp range=students policy=base1 ip=192.168.1.100 number=64
```

3. Configure a DHCP policy for the admin VLAN

```
create dhcp policy=base2 leasetime=7200
add dhcp policy=d subnet=255.255.255.0
add dhcp policy=base2 router=10.1.1.1
add dhcp policy=base2 dnsserver=172.16.1.254
create dhcp range=admin policy=base2 ip=10.1.1.100 number=32
```

PPPoE setup

1. Get a PPPoE client for the teachers' laptops

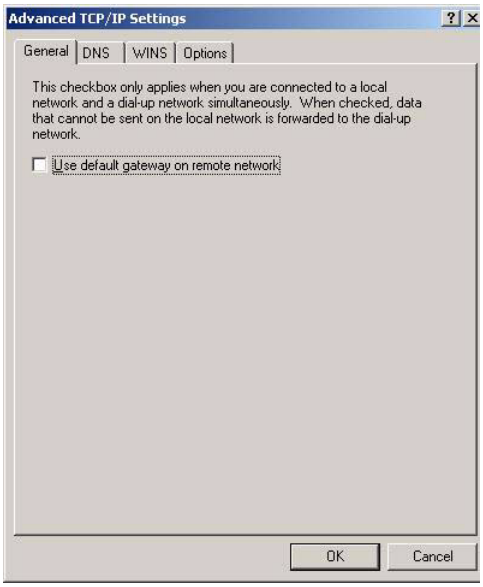
You can get information about PPPoE clients from www.carricksolutions.com/pppoe

We tested our solution using WinPoET. You can get details of this from www.finepoint.com/winpoet.html. WinPoET is used by many broadband providers who are presenting an Ethernet port solution, and has proved to be very reliable. Follow the manufacturers instructions to install the client.

2. Configure PPPoE client settings

When you have installed the PPPoE client, do the following to configure the correct settings:

1. Go to Settings > Network and Dialup Connections and click on **WinPoet connection**.
2. From the Eth WinPoet box, select **Properties**, then select the **Networking Tab**.
3. Select **Internet Protocol (TCP/IP)**, then select **Properties**.
4. Select **Advanced** and clear the 'Use default gateway on remote network' checkbox, as shown in the image below. This ensures that the default gateway the PC uses is the one for the Ethernet connection.



Note: We also found it useful to automatically add the dial-up icon in the task bar to show whether the connection was up or not.

3. Set up the PPPoE server on the switch

You can now set up the PPPoE server on your switch.

This configuration logs the user in, assign them an IP address and adds a dynamic PPP interface.

1. Create a template for the PPP link:

```
create ppp template=1
set ppp template=1 idle=600 bap=off authentication=chap
   mtu=1492 echo=10
```

   This sets up the PPP link with a 10 minute idle timer and CHAP authentication. We have also set the frame size smaller to prevent fragmentation.

2. Enable the Access concentrator to operate on the curriculum VLAN, and set up a PPP link using the template you created above:

```
add ppp acservice=teachers template=1 vlan=1
enable ppp accessconcentrator
```

3. Finally, add the users:

```
add user=teacher1 password=password login=no
```

   At this point you will be prompted for the login password for security. This is '*friend*'.

```
set user=teacher1 ipaddress=10.2.2.16 netmask=255.255.255.255
add user=teacher2 password=password login=no
set user=teacher2 ipaddress=10.2.2.17 netmask=255.255.255.255
```

   The above commands add two users, teacher1 and teacher2, and assign them the IP addresses 10.2.2.16 and 10.2.2.17 addresses with a host mask. You can add more users as required. Note that when you look at the configuration file, the passwords are encrypted for security.

Using RADIUS for user authentication

If there are a lot of teachers to add, the login can be backed off to a RADIUS server. This requires configuration of the RADIUS server location.

1. Specify the RADIUS server location

To specify the RADIUS server location, use the command:

```
add radius server=10.1.1.20 secret=valid8me
```

See your Software Reference for more information about RADIUS.

2. Test the PPPoE login

Now you can test the PPPoE login. Use a PC with the PPPoE client installed, connected to the curriculum network. Start the client, and login (using teacher1 and password in this example). Enter the following commands on the switch:

```
show ppp
```

```
show ip route
```

You should see a new PPP link come up, and a route to the new interface. On the PC, you can use the command **ipconfig** from a DOS window to see that the IP address was assigned. At this stage you will not see the admin VLAN, because of the firewall we set up earlier.

3. Save the configuration and clear dynamic PPP connections

Before going on to the next section, save your configuration, by using the commands:

```
create config=schoolfw.cfg
```

```
set config=schoolfw.cfg
```

Then we recommend rebooting the switch to clear any dynamic PPP connections.

Adding the PPPoE interfaces to the firewall

You need to set the dynamic PPPoE interfaces to be added on the private side of the firewall. This requires a dynamic firewall policy template to be set up, which is then used for setting the interfaces to be private.

1. Create a firewall policy template

First, configure a firewall policy template, with **users=any.** This means that any user will be added to that template.

```
create firewall policy=a dynamic=teachers
```

```
add firewall policy=a dynamic=teachers user=any
```

2. Add the template interfaces to the private side of the firewall

```
add firewall policy=a interface=dyn-teachers type=private
```

This has the effect that whenever a PPPoE connection is established to the switch, the PPP interface on the switch will be treated as being on the private side of the firewall. So, the PC client will effectively be on the private side of the firewall, and will have full access to all devices connected to VLAN 1 of the switch.

This gives a teacher the ability to connect to a VLAN 2 part of the switch but still get access to VLAN 1 (in behind the firewall).

3. Save the configuration

Finally, remember to save the configuration, and tell the switch to boot from this file next time using the commands:

```
create config=schoolfw.cfg
```

```
set config=schoolfw.cfg
```

To see the configuration, enter the command:

```
show config dynamic
```

Script-only configuration

This section provides a script-only version of the configuration. You can copy and paste the script below to your PC, then modify addresses, passwords and any other requirements for all your individual sites, and then use TFTP or ZMODEM to transfer the files to your routers. See the "Managing Configuration Files and Software Versions" chapter in your Software Reference for more information about TFTP and ZMODEM.

```
# SYSTEM configuration
set system name=school.firewall

# USER configuration
set user=manager pass=friend priv=manager lo=yes telnet=yes
add user=teacher1 pass=password lo=no ipaddr=10.2.2.16
set user=teacher1 netmask=255.255.255.255
add user=teacher2 pass=password lo=no
set user=teacher2 ipaddr=10.2.2.17 netmask=255.255.255.255

# PPP templates configuration
create ppp template=1
set ppp template=1 idle=600 bap=off authentication=chap mtu=1492 echo=10

# VLAN configuration
create vlan=admin vid=2
add vlan=admin port=17-24

# PPP configuration
add ppp acservice=teachers template=1 vlan=1
ena ppp accessconcentrator

# IP configuration
enable ip
add ip int=vlan1 ip=192.168.1.1 mask=255.255.255.0
add ip int=vlan2 ip=10.1.1.1 mask=255.255.255.0
add ip rou=0.0.0.0 mask=0.0.0.0 int=vlan1 next=192.168.1.254

# FIREWALL configuration
enable firewall
create firewall policy=a
create firewall policy=a dy=teachers
add firewall policy=a dy=teachers user=any
add firewall policy=a int=vlan2 type=private
add firewall policy=a int=dyn-teachers type=private
add firewall policy=a int=vlan1 type=public
add firewall poli=a nat=enhanced int=vlan2 gblin=vlan1

# DHCP configuration - Post IP
enable dhcp
create dhcp poli=base1 lease=7200
add dhcp poli=base1 subn=255.255.255.0 rou=192.168.1.1
add dhcp poli=base1 dnss=192.168.1.254
create dhcp poli=base2 lease=7200
add dhcp poli=base2 subn=255.255.255.0 rou=10.1.1.1
add dhcp poli=base2 dnss=172.16.1.254
create dhcp ran=admin poli=base2 ip=10.1.1.100 num=32
create dhcp ran=students poli=base1 ip=192.168.1.100 num=64
```

USA Headquarters | 19800 North Creek Parkway | Suite 200 | Bothell | WA 98011 | USA | T: +1 800 424 4284 | F: +1 425 481 3895
European Headquarters | Via Motta 24 | 6830 Chiasso | Switzerland | T: +41 91 69769.00 | F: +41 91 69769.11
Asia-Pacific Headquarters | 11 Tai Seng Link | Singapore | 534182 | T: +65 6383 3832 | F: +65 6383 3830
www.alliedtelesis.com

C613-16056-00 REV C