How To| Configure A Secure School Network Based On 802.1x

The problem

Schools offer a unique set of challenges to network designers. As well as all the usual requirements of modern network users—high bandwidth, resiliency, scalability—schools demand both stringent security and high flexibility.

Firstly, school network users are very mobile. Students and staff typically move between many locations in the course of a day, from classrooms to labs to libraries to dorm rooms.

Secondly, restricting physical access to network connection points is very difficult in such a mobile environment. Students, staff, and even members of the public frequently come and go from school buildings, and it is almost impossible to monitor all these people all the time. In spite of this, parts of the network must be kept secure. Staff must have access to certain network resources, particularly server drives, to which students must **not** have access. Students pose a constant threat to network security. They have the ability, time and often the inclination to probe for every weakness in the network's security set-up.

In other words, school networks take the often-discussed security *versus* flexibility dilemma to an extreme.

The solution

This How To Note describes a specific example of a highly reproducible school network solution from Allied Telesis.

Physically, the solution consists of AT-8624 switches on the edge with gigabit fibre uplinks back to a SwitchBlade in the core. But the real value in the network lies in the features that are implemented on these switches. In particular, the key requirements of simultaneous flexibility and security are provided by the 802.1x authentication process.

802.1x authentication and dynamic VLAN assignment prevent unauthorised access to the network while still giving users appropriate access to network resources, regardless of where they physically connect to the network. 802.1x authentication ensures that users cannot even send packets into the network until they have provided valid authentication credentials. VLAN assignment puts authenticated users into an appropriate VLAN, based on their authentication credentials. Therefore users experience the same network environment no matter where they connect from.

Another key part of the solution is hardware filtering on the SwitchBlade. Hardware filters guarantee no leakage of traffic between certain IP subnets, and achieve this with no degradation of data throughput.

What information will you find in this document?

The rest of this How To Note describes the network configuration in the following sections:

Which products and software version does it apply to?

The core of the network is a SwitchBlade, running Software Version 2.7.5a. Alternatively, you can use an AT-9900 series switch in the core.

The edge switches can be any of:

- AT-8600 series switches (recommended)
- AT-8700XL series switches
- Rapier and Rapier i series switches
- AT-8800 series switches
- AT-8948 switches
- AT-9900 series switch
- x900-48 series switch

The edge switches run Software Version 2.7.5 or later.

Related How To Notes

How To Configure A Secure Network Solution For Schools describes an alternative approach. It uses a firewall to stop students from accessing staff resources. This solution does not offer security for mobile users.

How To Use 802.1x EAP-TLS Or PEAP-MS-CHAP v2 With Microsoft® Windows® Server 2003 To Make A Secure Network describes how to set up Microsoft servers and clients for authentication through an 802.1x-compatible Allied Telesis switch.

How to use 802.1x VLAN assignment and *How To Configure MAC-based port authentication* give more information about port authentication.

How to set up a RADIUS server for user authentication describes RADIUS servers, including server redundancy.

How To Notes are available from www.alliedtelesis.com/resources/literature/howto.aspx and may be found in the Resource Center on the Documentation and Tools CD-ROM that is shipped with your switch.

Details of the network

The VLANs

The network consists of 9 VLANs. Some of the VLANs reach right out to the edge of the network, and some are confined just to the core. The VLANs are:

- **secondary-clients** (VID=10) and **primary-clients** (VID=100)

  The two staff VLANS, one each for the Secondary School staff and Primary School staff. These VLANs reach to the edge of the network, and staff members are placed into one or other of these VLANS, based on their user IDs.

- **secondary-servers** (VID=20)

  The VLAN that contains the Senior School servers. This VLAN has to extend to the uplink port of each edge switch, because it includes the RADIUS servers used by 802.1x.

- **primary-servers** (VID=120)

  The VLAN that contains the Junior School servers. This VLAN is constrained just to the core of the network.

- **secondary-printers** (VID=30) and **primary-printers** (VID=130)

  The two VLANs that contain the printers for the Senior School and Junior School. These VLANs are constrained just to the core of the network.

- **student** (VID=50)

  The VLAN into which 802.1x places students when they connect. This VLAN gives them access to nothing but the students' server. It reaches to the edge of the network.

- **firewall** (VID=5)

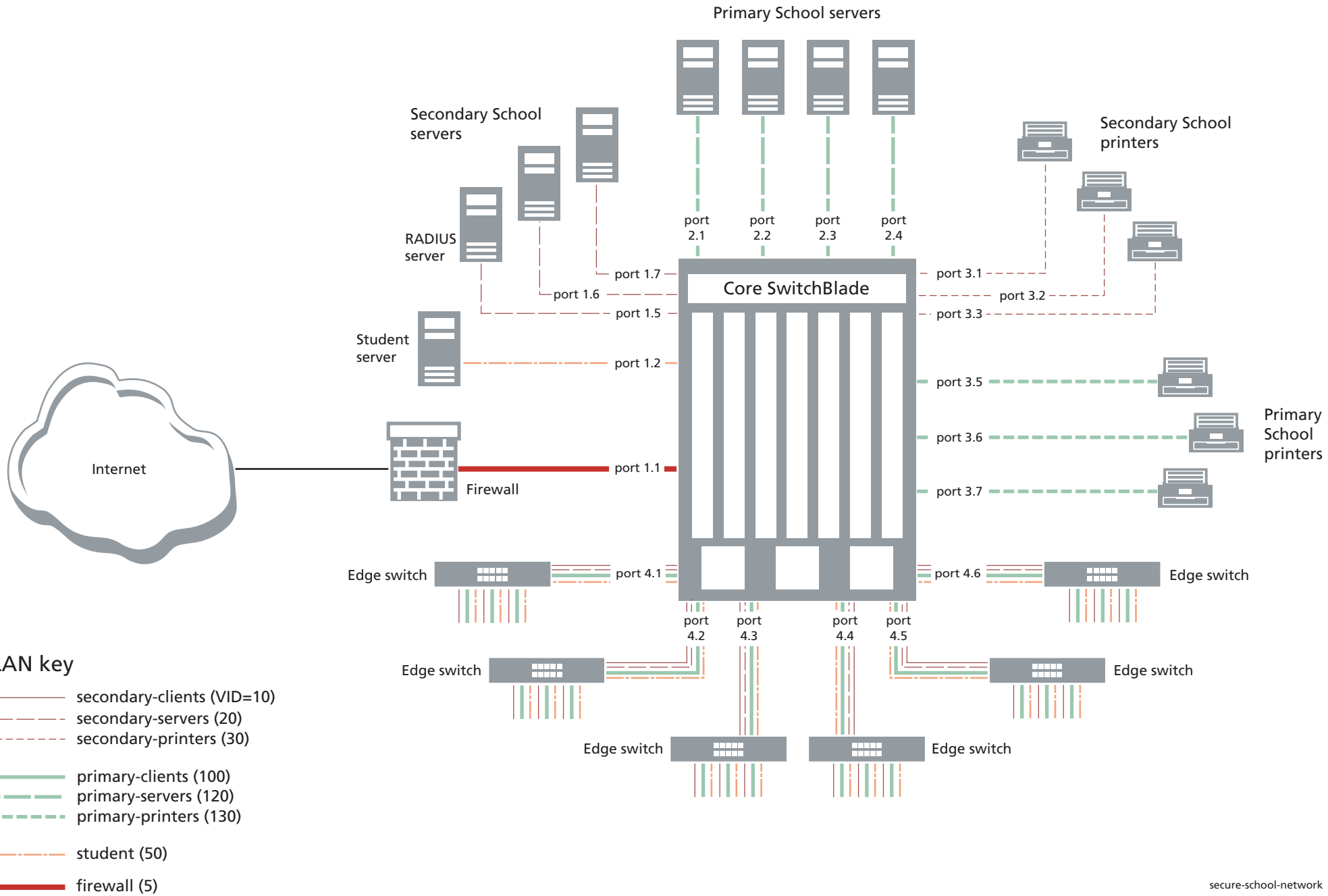
  The VLAN that contains the firewall, to provide access from the network out to the Internet.

- **untrusted** (VID=500)

  The guest VLAN that ports reside in by default (except for the ports that are permanently reserved for servers, printers, edge switches, the firewall, and the uplink from an edge switch to the core). When a port receives valid authentication credentials, it is taken from this VLAN and put into the VLAN relevant to the person who has just been authenticated on the port.

The next page shows a diagram of the network. Note that the diagram doesn't show the untrusted VLAN because the only ports that are permanently in the untrusted VLAN are ports that are not in any other VLAN.

One advantage of using a SwitchBlade is its modularity. The wide range of line cards available for SwitchBlades offers many different combinations of ports. This means you can buy the ports you currently need and easily expand as your network expands. This example uses four 8-port line cards.


Primary School servers
Secondary School servers
Secondary School printers
RADIUS server
Student server
Internet
Firewall
Core SwitchBlade
port 1.1
port 1.2
port 1.5
port 1.6
port 1.7
port 2.1
port 2.2
port 2.3
port 2.4
port 3.1
port 3.2
port 3.3
port 3.5
port 3.6
port 3.7
Primary School printers
Edge switch
port 4.1
port 4.2
port 4.3
port 4.4
port 4.5
port 4.6
Edge switch
Edge switch
Edge switch
Edge switch
VLAN key
secondary-clients (VID=10)
secondary-servers (20)
secondary-printers (30)
primary-clients (100)
primary-servers (120)
primary-printers (130)
student (50)
firewall (5)
secure-school-network

Communication between the VLANs

This example strictly controls whether hosts in different VLANs can communicate with each other. The untrusted VLAN cannot send data, so in effect it cannot communicate with any other VLAN. The table below shows which of the other VLANs can (Y) and cannot (-) communicate with each other. It also shows each VLAN's IP subnet.

VLAN details	**secondary-clients**	**secondary-servers**	**secondary-printers**	**primary-clients**	**primary-servers**	**primary-printers**	**student**	**firewall**
secondary-clients 192.168.10.0		Y	-	-	-	-	-	Y
secondary-servers 192.168.20.0	Y		Y	-	Y	-	-	-
secondary-printers 192.168.30.0	-	Y		-	-	-	-	-
primary-clients 192.168.100.0	-	-	-		Y	-	-	Y
primary-servers 192.168.120.0	-	Y	-	Y		Y	-	-
primary-printers 192.168.130.0	-	-	-	-	Y		-	-
student 192.168.50.0	-	-	-	-	-	-		Y
firewall 192.168.5.0	Y	-	-	Y	-	-	Y	

To create the above restrictions, this configuration does the following:

- On the core SwitchBlade, a set of hardware filters block communication between the IP subnets used on different VLANs.
- On the edge switches, inter-VLAN communication does not need to be blocked by filters. This is because 802.1x puts the edge ports of those switches into one of only three possible VLANS—primary-clients, secondary-clients or student—and these VLANs do not have Layer 3 interfaces on the edge switches. There is no possibility of Layer 3 switching between them.

  However, a different restriction is necessary on the edge switches: there must be no communication at all between different hosts in the student VLAN, to stop students from looking at each other's accounts. This restriction cannot be achieved by configuring the student VLAN as a private VLAN, because standard private VLANs are incompatible with allocating the ports by 802.1x. Instead, this configuration uses a clever set of L3 filters to block any traffic in the student VLAN between pairs of edge ports, and to force broadcast/multicast packets in the student VLAN up to the network core.

Edge Switch Configuration

Enter the following configuration on each edge switch.

1. Configure the switch's time

Use NTP to get the correct time from a time server.

```
enable ntp
add ntp peer=172.16.249.54
```

Automatically change the time when summertime (daylight saving) starts and ends. This example uses British Summer Time.

```
enable summertime
set summertime=bst startmonth=mar startweek=5 starttime=01:00:00
  endmonth=oct endweek=5 endtime=01:00:00
```

The value 5 for **startweek** and **endweek** means the last week in the month.

2. Configure the uplink port

```
set switch port=25 description=Uplink
set switch port=25 acceptable=vlan
```

3. Create the VLANs

Create the 3 VLANs for staff and students.

```
create vlan=secondary-clients vid=10
create vlan=primary-clients vid=100
create vlan=student vid=50
```

Create the secondary-servers VLAN. This VLAN needs to extend to the uplink port of the edge switches because it contains the RADIUS servers that 802.1x uses.

```
create vlan=secondary-servers vid=20
```

Create the untrusted VLAN. This VLAN is just a placeholder VLAN that edge ports are allocated to when no user is connected.

```
create vlan=untrusted vid=500
```

4. Put ports into the VLANs

```
add vlan=500 port=1-24
add vlan=20 port=25 frame=tagged
add vlan=10 port=25 frame=tagged
add vlan=100 port=25 frame=tagged
add vlan=50 port=25 frame=tagged
```

Remove the uplink port from the default VLAN.

```
delete vlan=1 port=25
```

5. Create classifiers to match packets in the student VLAN

Create classifiers to match packets in the student VLAN that enter the switch via the edge ports.

```
create classifier=1 iport=1 vlan=50
create classifier=2 iport=2 vlan=50
create classifier=3 iport=3 vlan=50
create classifier=4 iport=4 vlan=50
create classifier=5 iport=5 vlan=50
create classifier=6 iport=6 vlan=50
create classifier=7 iport=7 vlan=50
create classifier=8 iport=8 vlan=50
create classifier=9 iport=9 vlan=50
create classifier=10 iport=10 vlan=50
create classifier=11 iport=11 vlan=50
create classifier=12 iport=12 vlan=50
create classifier=13 iport=13 vlan=50
create classifier=14 iport=14 vlan=50
create classifier=15 iport=15 vlan=50
create classifier=16 iport=16 vlan=50
create classifier=17 iport=17 vlan=50
create classifier=18 iport=18 vlan=50
create classifier=19 iport=19 vlan=50
create classifier=20 iport=20 vlan=50
create classifier=21 iport=21 vlan=50
create classifier=22 iport=22 vlan=50
create classifier=23 iport=23 vlan=50
create classifier=24 iport=24 vlan=50
```

Create a classifier to match all packets in the student VLAN.

```
create classifier=100 vlan=50
```

Create classifiers to match packets in the student VLAN that enter and leave the switch via the uplink port.

```
create classifier=101 iport=25 vlan=50
create classifier=102 eport=25 vlan=50
```

6. Create filters to discard or redirect packets in the student VLAN

Make a filter to mark all student VLAN packets for discard.

```
add switch hwfilter classifier=100 action=discard
```

Make filters for broadcasts and multicasts that enter the student VLAN via the edge ports, and for packets that are destined for the uplink port.

```
add switch hwfilter classifier=1-24
  action=sendnonunicasttoport,nodrop,sendeport port=25
```

The above filters send matching packets to the uplink port, instead of discarding them. They achieve this by the following actions:

- **sendnonunicasttoport** sends multicast and broadcast packets to port 25.
- **nodrop** and **sendeport** together stop the switch from discarding packets that are destined for port 25 and came from the classifier's port (ports 1-24 for classifiers 1-24)

Make filters to avoid discarding student VLAN packets that enter or leave the switch via the uplink port.

```
add switch hwfilter classifier=101 action=nodrop
add switch hwfilter classifier=102 action=nodrop
```

7. Assign an IP address to the secondary-servers VLAN

The switch uses this address for RADIUS communication. Note that each edge switch must have a different IP address.

```
enable ip
add ip int=vlan20 ip=192.168.20.200
add ip rou=0.0.0.0 mask=0.0.0.0 int=vlan20 next=192.168.20.254
```

8. Configure port authentication

```
enable portauth=macbased
enable portauth=macbased port=1-24
```

This configuration uses MAC-based authentication on the edge switches. This lets you connect legacy PCs that do not support 802.1x. If all your PCs are 802.1x capable, we recommend you use 802.1x instead, because it is harder to spoof.

Note that it is possible to use 802.1x with Windows 2000, but support is not enabled by default. See the Microsoft article *Using 802.1x authentication on client computers that are running Windows 2000*.

To get step by step instructions for setting up Microsoft clients and servers to use 802.1x authentication, see *How To Use 802.1x EAP-TLS Or PEAP-MS-CHAP v2 With Microsoft® Windows® Server 2003 To Make A Secure Network*. This Allied Telesis How To Note is available from www.alliedtelesis.com/resources/literature/howto.aspx..

Core Switch Configuration

Enter the following configuration on the SwitchBlade.

1. Configure the switch's location and time

Name the switch after the school.

```
set system name=Hogwarts
```

Use NTP to get the correct time from a time server.

```
enable ntp
add ntp peer=172.16.249.54
```

Automatically change the time when summertime (daylight saving) starts and ends. This example uses British Summer Time.

```
enable summertime
set summertime=BST startmonth=mar startweek=5 starttime=01:00:00
  endmonth=oct endweek=5 endtime=01:00:00
```

2. Configure the ports

```
set switch port=4.1 description=Gryffindor
set switch port=4.2 description=Hufflepuff
set switch port=4.3 description=Slytherin
set switch port=4.4 description="Ravenclaw (IT Suite)"
set switch port=4.5 description="Ravenclaw (Tower)"
set switch port=4.6 description=Library
```

3. Create the VLANs

```
create vlan=firewall vid=5
create vlan=secondary-clients vid=10
create vlan=secondary-servers vid=20
create vlan=secondary-printers vid=30
create vlan=primary-clients vid=100
create vlan=primary-servers vid=120
create vlan=primary-printers vid=130
create vlan=student vid=50
create vlan=untrusted vid=500
```

4. Put ports into the VLANs

firewall:

```
add vlan=5 port=1.1
```

secondary-clients:

```
add vlan=10 port=4.1-4.6 frame=tagged
```

secondary-servers:

```
add vlan=20 port=1.5-1.7
add vlan=20 port=4.1-4.6 frame=tagged
```

secondary-printers:

```
add vlan=30 port=3.1-3.3
```

primary-clients:

```
add vlan=100 port=4.1-4.6 frame=tagged
```

primary-servers:

```
add vlan=120 port=2.1-2.4
```

primary-printers:

```
add vlan=130 port=3.5-3.7
```

student:

```
add vlan=50 port=1.2
add vlan=50 port=4.1-4.6 frame=tagged
```

untrusted:

```
add vlan=500 port=1.3-1.4,1.8,2.5-2.8,3.4,3.8,4.7-4.8
```

Putting the unused ports into the untrusted VLAN increases security. If an unauthorised user gets access to the SwitchBlade and plugs a device into an unused port, they get no access to the network. It also means that you can connect authorised users to these ports and use 802.1x to assign them to VLANs.

Also, remove ports 4.1-4.6 from the default VLAN. These ports connect to the edge switches and should not be untagged members of any VLAN.

```
delete vlan=1 port=4.1-4.6
```

5. Create classifiers

This configuration stops most VLANs from communicating with each other, by discarding packets. To identify packets that need to be discarded, create the following classifiers. The classifiers check IP addresses and match packets between pairs of VLANs that must not communicate.

```
cre class=1 prot=ip ipsa=192.168.120.0/24 ipda=192.168.10.0/24
cre class=2 prot=ip ipsa=192.168.120.0/24 ipda=192.168.30.0/24
cre class=3 prot=ip ipsa=192.168.120.0/24 ipda=192.168.5.0/24
cre class=4 prot=ip ipsa=192.168.120.0/24 ipda=192.168.50.0/24
cre class=5 prot=ip ipsa=192.168.20.0/24 ipda=192.168.130.0/24
```

```
cre class=6 prot=ip ipsa=192.168.20.0/24 ipda=192.168.100.0/24
cre class=7 prot=ip ipsa=192.168.20.0/24 ipda=192.168.5.0/24
cre class=8 prot=ip ipsa=192.168.20.0/24 ipda=192.168.50.0/24
cre class=9 prot=ip ipsa=192.168.10.0/24 ipda=192.168.120.0/24
cre class=10 prot=ip ipsa=192.168.10.0/24 ipda=192.168.30.0/24
cre class=11 prot=ip ipsa=192.168.10.0/24 ipda=192.168.100.0/24
cre class=12 prot=ip ipsa=192.168.10.0/24 ipda=192.168.130.0/24
cre class=13 prot=ip ipsa=192.168.10.0/24 ipda=192.168.50.0/24
cre class=14 prot=ip ipsa=192.168.30.0/24 ipda=192.168.120.0/24
cre class=15 prot=ip ipsa=192.168.30.0/24 ipda=192.168.10.0/24
cre class=16 prot=ip ipsa=192.168.30.0/24 ipda=192.168.100.0/24
cre class=17 prot=ip ipsa=192.168.30.0/24 ipda=192.168.130.0/24
cre class=18 prot=ip ipsa=192.168.30.0/24 ipda=192.168.5.0/24
cre class=19 prot=ip ipsa=192.168.30.0/24 ipda=192.168.50.0/24
cre class=20 prot=ip ipsa=192.168.100.0/24 ipda=192.168.10.0/24
cre class=21 prot=ip ipsa=192.168.100.0/24 ipda=192.168.30.0/24
cre class=22 prot=ip ipsa=192.168.100.0/24 ipda=192.168.130.0/24
cre class=23 prot=ip ipsa=192.168.100.0/24 ipda=192.168.20.0/24
cre class=24 prot=ip ipsa=192.168.100.0/24 ipda=192.168.50.0/24
cre class=25 prot=ip ipsa=192.168.130.0/24 ipda=192.168.20.0/24
cre class=26 prot=ip ipsa=192.168.130.0/24 ipda=192.168.10.0/24
cre class=27 prot=ip ipsa=192.168.130.0/24 ipda=192.168.30.0/24
cre class=28 prot=ip ipsa=192.168.130.0/24 ipda=192.168.100.0/24
cre class=29 prot=ip ipsa=192.168.130.0/24 ipda=192.168.5.0/24
cre class=30 prot=ip ipsa=192.168.130.0/24 ipda=192.168.50.0/24
cre class=31 prot=ip ipsa=192.168.50.0/24 ipda=192.168.20.0/24
cre class=32 prot=ip ipsa=192.168.50.0/24 ipda=192.168.120.0/24
cre class=33 prot=ip ipsa=192.168.50.0/24 ipda=192.168.30.0/24
cre class=34 prot=ip ipsa=192.168.50.0/24 ipda=192.168.10.0/24
cre class=35 prot=ip ipsa=192.168.50.0/24 ipda=192.168.100.0/24
cre class=36 prot=ip ipsa=192.168.50.0/24 ipda=192.168.130.0/24
```

Also create classifiers to match other traffic that must be forwarded. For example, this classifier matches DHCP packets:

```
create classifier=100 udpd=67
```

6. Assign IP addresses to the VLANs

```
enable ip
add ip int=vlan5 ip=192.168.5.254
add ip int=vlan10 ip=192.168.10.254
add ip int=vlan20 ip=192.168.20.254
add ip int=vlan30 ip=192.168.30.254
add ip int=vlan100 ip=192.168.100.254
add ip int=vlan120 ip=192.168.120.254
add ip int=vlan130 ip=192.168.130.254
add ip int=vlan50 ip=192.168.50.254
add ip route=0.0.0.0 mask=0.0.0.0 int=vlan5 next=192.168.5.1
```

7. Create a hardware filter

Add a filter entry to forward DHCP packets.

```
add switch hwfilter=1 classifier=100 action=forward dport=all
```

Add filter entries to discard packets between pairs of VLANs that must not communicate.

```
add switch hwfilter=1 classifier=1-36 action=discard dport=all
```

Notes:

1. This solution applies hardware filters to all ports on the SwitchBlade and may need to be modified for networks that use a large number of ports. If this applies to you, please contact your Allied Telesis representative for more information.
2. If you use an AT-9900 series switch instead of the SwitchBlade, make a hardware filter for each classifier.

8. Specify the RADIUS servers for port authentication to use

The SwitchBlade can access two RADIUS servers, which provides redundancy if one server goes down. For more information, including how to set up redundant servers, see *How To Set Up A RADIUS Server For User Authentication*. This How To Note is available from www.alliedtelesis.com/resources/literature/howto.aspx.

```
add radius server=192.168.20.5 secret=secret-password
add radius server=192.168.20.6 secret=secret-password
```

9. Configure port authentication

Enable port authentication on the unused ports. This increases security by ensuring that only devices with valid authentication credentials can connect to these ports.

```
enable portauth=8021x

enable portauth=8021x port=1.3-1.4,1.8,2.5-2.8,3.4,3.8,4.7-4.8
  type=authenticator quietperiod=0 txperiod=1 servertimeout=5
```

To get step by step instructions for setting up Microsoft clients and servers to use 802.1x authentication, see *How To Use 802.1x EAP-TLS Or PEAP-MS-CHAP v2 With Microsoft® Windows® Server 2003 To Make A Secure Network*. This How To Note is available from www.alliedtelesis.com/resources/literature/howto.aspx.

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

C613-16089-00 REV B