APPENDIX A  VLAN Design and Configuration

A.1 VLAN Configuration Example 1

The first example configuration is a simple VLAN implementation where all the ports configured in the Net2 System VLAN (VLAN 2) reside on the same 3Com switch. In this configuration no trunking of the Net2 System VLAN is required. Inter-VLAN routing is also unnecessary as the Net2 Server has LAN adapters in both VLANs (There are only two VLANs, the Net2 System VLAN and the default management VLAN). Having the Net2 System VLAN restricted to one switch has the added benefit of keeping the Net2 System VLAN traffic off the backbone, which in this instance is the 3Com 4924 core switch backplane.

A.1.1 IP addressing scheme

The Net2 Server, Net2 Clients and all the Net2 485 TCP/IP devices should be configured with IP addresses in the same subnet and attached to switch ports assigned to the Net2 System VLAN (VLAN 2 in this example). See fig A.1
Sample 3Com VLAN Configuration for Connecting Paxton Net2 System Devices to a Small Office Network

A.1.2 3Com 4200 Access Switch Configuration

In this example the 4200 is the only switch that needs to be configured for VLANs
A.1.2.1 Define VLAN 2 as the Net2 VLAN

Switch menu>bridge>vlan>create>2

Name the VLAN
Switch menu>bridge>vlan>modify>name>2>Net2 System

Check VLAN config
Switch menu>bridge>vlan>summary all

4200 CLI Output:

Select menu option (bridge/vlan): summary all

<table>
<thead>
<tr>
<th>VLAN ID</th>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>1*</td>
<td>Default VLAN</td>
</tr>
<tr>
<td>2</td>
<td>Net2 System</td>
</tr>
</tbody>
</table>

* indicates management VLAN (Not configurable)

A.1.2.1 Configure the ports:

This can also be done on the web browser interface

Set port and duplex settings

The first two ports are configured for the 485 TCP/IP converters

Port 1:1

Disable autonegotiation and set the port to 10Mbps half duplex:
Switch menu>physicalInterface>ethernet>portMode>1:1>disable>10half

Port 1:2

Disable autonegotiation and set the port to 10Mbps half duplex:
Switch menu>physicalInterface>ethernet>portMode>1:2>disable>10half

Port 1:3

The Netgear radio unit can connect at 10/100Mbps at full-duplex or half-duplex.

enable autonegotiation and set the port to fallback to 100Mbps full duplex:
Switch menu>physicalInterface>ethernet>portMode>1:3>enable>100full
Port 1:4

The Net2 Server can connect at 10/100Mbps at full-duplex or half-duplex.

enable autonegotiation and set the port to fallback to 100Mbps full duplex:  
Switch menu>physicalInterface>ethernet>portMode>1:25>enable>100full

Port 1:25

The Net2 server can connect at 10/100/1000 Mbps at full-duplex or half-duplex

enable autonegotiation and set the port to fallback to 1000Mbps full duplex:  
Switch Menu>physicalInterface>ethernet>portMode>1:25>enable>1000full

Check the configuration:  
Switch menu>physicalInterface>ethernet>summary 1:1,1:2,1:3,1:4,1:25

Refresh Time:10 Second

<table>
<thead>
<tr>
<th>Port State</th>
<th>Mode</th>
<th>Rx Packets</th>
<th>Rx Octets</th>
<th>Errors</th>
</tr>
</thead>
<tbody>
<tr>
<td>1:1 enabled</td>
<td>10half</td>
<td>45838501</td>
<td>3932145667</td>
<td>0</td>
</tr>
<tr>
<td>1:2 enabled</td>
<td>10half</td>
<td>1665867</td>
<td>268143841</td>
<td>0</td>
</tr>
<tr>
<td>1:3 enabled</td>
<td>100full (Auto)</td>
<td>27180807</td>
<td>2985484437</td>
<td>0</td>
</tr>
<tr>
<td>1:4 enabled</td>
<td>100full (Auto)</td>
<td>78665</td>
<td>8147560</td>
<td>0</td>
</tr>
<tr>
<td>1:25 enabled</td>
<td>1000full (Auto)</td>
<td>17420</td>
<td>1818436</td>
<td>0</td>
</tr>
</tbody>
</table>

Add ports 1:1, 1:2, 1:3, and 1:4 to VLAN 2

Switch menu>bridge>vlan>modify>addPort>2>1:1>untagged (non-trunking)  
Switch menu>bridge>vlan>modify>addPort>2>1:2>untagged (non-trunking)  
Switch menu>bridge>vlan>modify>addPort>2>1:3>untagged (non-trunking)  
Switch menu>bridge>vlan>modify>addPort>2>1:4>untagged (non-trunking)

Check the configuration:  
Switch menu>bridge>vlan>detail all

Type "quit" to return to the previous menu or  ? for help

-----------------------------3COM 24 Port Switch (1)-----------------------------
Select menu option (bridge/vlan): detail all

VLAN ID: 1 Name: Default VLAN

<table>
<thead>
<tr>
<th>Unit</th>
<th>Untagged Member Ports</th>
<th>Tagged Member Ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>5-26</td>
<td>none</td>
</tr>
<tr>
<td></td>
<td>Aggregated Links AL1-AL4</td>
<td>none</td>
</tr>
</tbody>
</table>
VLAN ID: 2      Name: Net2 System

<table>
<thead>
<tr>
<th>Unit</th>
<th>Untagged Member Ports</th>
<th>Tagged Member Ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1-4</td>
<td>none</td>
</tr>
</tbody>
</table>

Aggregated Links  none    none

A.1.2.2   STP tuning

Separate instances of STP for VLANs (MSTP) is not supported on the Paxton house switches, however as all the Net2 System devices are end nodes they can be put in stpFastStart mode and will therefore not participate in a Spanning Tree

Force end stations in VLAN 2 to remain forwarding during STP convergence

Switch menu>bridge>port>stpFastStart>1:1
Switch menu>bridge>port>stpFastStart>1:2
Switch menu>bridge>port>stpFastStart>1:3
Switch menu>bridge>port>stpFastStart>1:4

A.2 VLAN Configuration Example 2

The second more complex example configuration employs Cisco Switches and is more typical of an Enterprise network [GT-check collapsed backbone] (see Fig A.2 below). The two core switches are configured as VLAN Trunking Protocol (VTP) Servers, one of them as the primary server (The first switch to be configured as a VTP Server becomes the VTP Primary Server) and the other as a secondary server for resilience. The Primary Server maintains a database of all VLANs in its domain and propagates database updates to any VTP Clients configured in the same domain. VLAN administration happens exclusively on the VTP Primary Domain Server.

Both core switches have dual backbone trunk links that must be configured to trunk all the VLANs that span the core. Their access trunk links must be similarly configured to trunk these VLANs

The access switches must be configured in VTP Client mode and their links to the core switches must also be configured to trunk all VLANs that span the network. Finally the access ports to end stations such as workstations, servers and Net2 485 TCP/IP devices must be assigned VLAN ids.

A.2.1 IP Addressing Scheme

The Net2 Server, Net2 Clients and all the Net2 485 TCP/IP devices should be configured with IP addresses in the same subnet and attached to switch ports assigned
to the same VLAN id (VLAN 3 in the example). This will simplify the configuration of the network and no Inter-VLAN routing will be required for the Net2 system to operate. However if any of the Net2 components are on different networks or VLANs, they will require routing to communicate.

Sample Cisco VLAN Configuration for Connecting Paxton Net2 System Devices to an Enterprise Network

Sample IP Addressing Scheme

<table>
<thead>
<tr>
<th>VLAN</th>
<th>IP Address</th>
<th>VLAN</th>
<th>IP Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>192.168.10.0</td>
<td>3</td>
<td>192.168.11.0</td>
</tr>
<tr>
<td>Net2 Server: 192.168.10.2</td>
<td>Workstation 1: 192.168.11.3</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Net2 Client: 192.168.10.3</td>
<td>Workstation 2: 192.168.11.4</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Port speed abbreviations

- Fa0/3: 10/100 Mbps on Module 0, port 3
- Gi1/2: 1000 Mbps on Module 1, port 2

Fig A2

A.2.2 Core Catalyst 6500 Series Configuration.
These switches are running the Cisco CatOS and the command sets are CLI commands.

The VLAN configuration is identical for both core switches with the exception of the VTP mode. The first switch to be configured as the VTP Server becomes the primary VTP Domain Server. If the second core switch is configured in VTP Server mode it becomes the Secondary Domain Server for resilience. VLAN administration, including the creation, addition and deletion of all VLANs is performed on the VTP Primary Server and the updates automatically sent to the VTP Clients.

A.2.2.1 Configure the VTP server:

CatOSSwitch (enable)> set vtp domain EndClientDomain mode server

A.2.2.2 Define the VLANs (on the Primary VTP Server)

The first Core Switch configured in Server mode will become the designated domain server. Others can also be configured as Servers for resilience:

CatOSSwitch (enable)> set vlan 2 ** End Client Workgroup VLAN **
CatOSSwitch (enable)> set vlan 3 ** VLAN for Net2 Paxton Access devices **

A.2.2.3 Configure the Backbone Gigabit Trunks:

NOTE: The convention used on Cisco devices to identify modules and ports in their command set (IOS and CatOS) is module/port, i.e. 1/1 is module 1, port 1

Configure the VLAN trunks using 802.1q encapsulation

CatOSSwitch (enable)> set trunk 1/3 nonegotiate dot1q
CatOSSwitch (enable)> set trunk 1/4 nonegotiate dot1q

Specify which VLANs are to be trunked.

By default all VLANs are trunked. These are VLANs 1 to 1005. VLAN 1 is the management VLAN and should never be removed. On Cisco switches, the usual practice is to clear all the VLANs on the trunk and then add back those you wish to trunk. Since VLAN 1 is the management VLAN and we are only trunking VLANs 2 and 3, all we need to do is remove the rest, i.e. 4-1005:

CatOSSwitch (enable)> clear trunk 1/3 4-1005
CatOSSwitch (enable)> clear trunk 1/4 4-1005

Now use the show trunk command to check the configuration and save it:
**NOTE:** In normal operation Spanning Tree will put one of the backbone links into blocking mode to stop loops. However, Cisco has a command set on high end switches to load balance VLANs over both trunks with prioritisation of traffic and without compromising Spanning Tree. The configuration of this is beyond the scope of this document. See section on Spanning Tree.

### A.2.2.4 Configure the Access Gigabit Trunks:

This is essentially the same as for the backbone trunks. Only the port specifications are different:

CatOSSwitch (enable)> set trunk 1/1 nonegotiate dot1q  
CatOSSwitch (enable)> set trunk 1/2 nonegotiate dot1q

**Specify which VLANs are to be trunked.**

By default all VLANs are trunked. These are VLANs 1 to 1005. VLAN 1 is the management VLAN and should never be removed. On Cisco switches, the usual practice is to clear all the VLANs on the trunk and then add back those you wish to trunk. Since VLAN 1 is the management VLAN and we are only trunking VLANs 2 and 3, all we need to do is remove the rest, i.e. 4-1005:

CatOSSwitch (enable)> clear trunk 1/1 4-1005  
CatOSSwitch (enable)> clear trunk 1/2 4-1005

Now use the show trunk command to check the configuration and save it:

CatOSSwitch (enable)> show trunk 1/1  
CatOSSwitch (enable)> show trunk 1/2

### A.2.3 Access Catalyst 4500 series configuration.

These switches are running the Cisco CatOS and the command sets are CLI commands. The VLAN configuration is identical for both Access Switches.

#### A.2.3.1 Set the VTP mode:

VTP is the VLAN Trunking Protocol and is used to maintain VLAN database consistency across trunk links. The access switches are configured as VTP Clients in the same domain as the VTP Server.
The access switches are configured as Clients and learn about the VLANs from the VTP Server.

**A.2.3.2 Configure VLAN port membership on the Fast Ethernet access ports**

NOTE: The convention used on Cisco devices to identify modules and ports in their command set (IOS and CatOS) is module/port, i.e. 1/1 is module 1, port 1

CatOSSwitch (enable)> set vlan 2 0/1 ** Net2 485 TCP/IP device **
CatOSSwitch (enable)> set vlan 3 0/2 ** End Client Workstation **
CatOSSwitch (enable)> set vlan 3 0/3 ** Net2 Client or Server **

**A.2.3 Configure the Gigabit Ethernet trunk uplinks**

Enable VLAN trunking over the Gigabit uplink to core switches using 802.1q encapsulation (enables VLAN frame tagging):

CatOSSwitch (enable)> set trunk 1/1 nonegotiate dot1q
CatOSSwitch (enable)> set trunk 1/2 nonegotiate dot1q

**Specify which VLANs are to be trunked.**

By default all VLANs are trunked. These are VLANs 1 to 1005. VLAN 1 is the management VLAN and should never be removed. On Cisco switches, the usual practice is to clear all the VLANs on the trunk and then add back those you wish to trunk. Since VLAN 1 is the management VLAN and we are only trunking VLANs 2 and 3, all we need to do is remove the rest, i.e. 4-1005:

CatOSSwitch (enable)> clear trunk 1/1 4-1005
CatOSSwitch (enable)> clear trunk 1/2 4-1005

Now use the show trunk command to check the configuration and save it:

CatOSSwitch (enable)> show trunk 1/1
CatOSSwitch (enable)> show trunk 1/2

**A.2.4 STP tuning**

With Cisco switches portfast can be configured on end nodes. End devices, like workstations, are devices which have no other network connections and therefore cannot introduce loops in the network. Portfast speeds up the convergence of Spanning Tree and puts the port into a forwarding state immediately.
CatOSSwitch (enable)> set spantree portfast 0/1 enable
CatOSSwitch (enable)> set spantree portfast 0/2 enable
CatOSSwitch (enable)> set spantree portfast 0/3 enable