Configuration Examples

Asymmetric VLAN and Traffic Segmentation

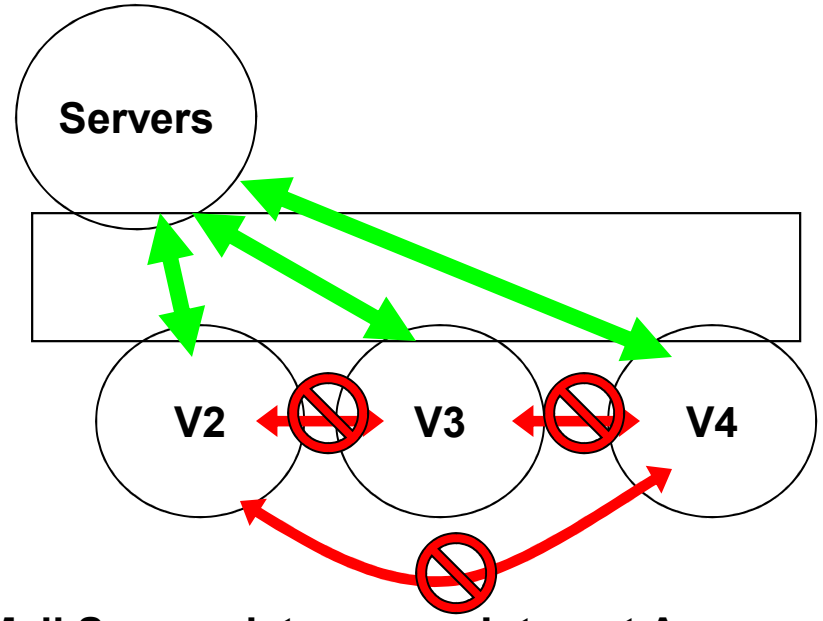
For Shared Server Application using L2 switch

Technical Support Division

D-Link ME

May 2008

Shared Server/Shared Internet Access Application



- Shared Servers (Mail Server, data server, Internet Access servers) can be access by all user groups, but the access between groups are not allowed (for the performance or security consideration)
- L2 solution: Asymmetric VLAN or Traffic Segmentation
- L3 solution: L3 switch + ACL to limit the access between group.

Asymmetric VLAN vs. Traffic Segmentation

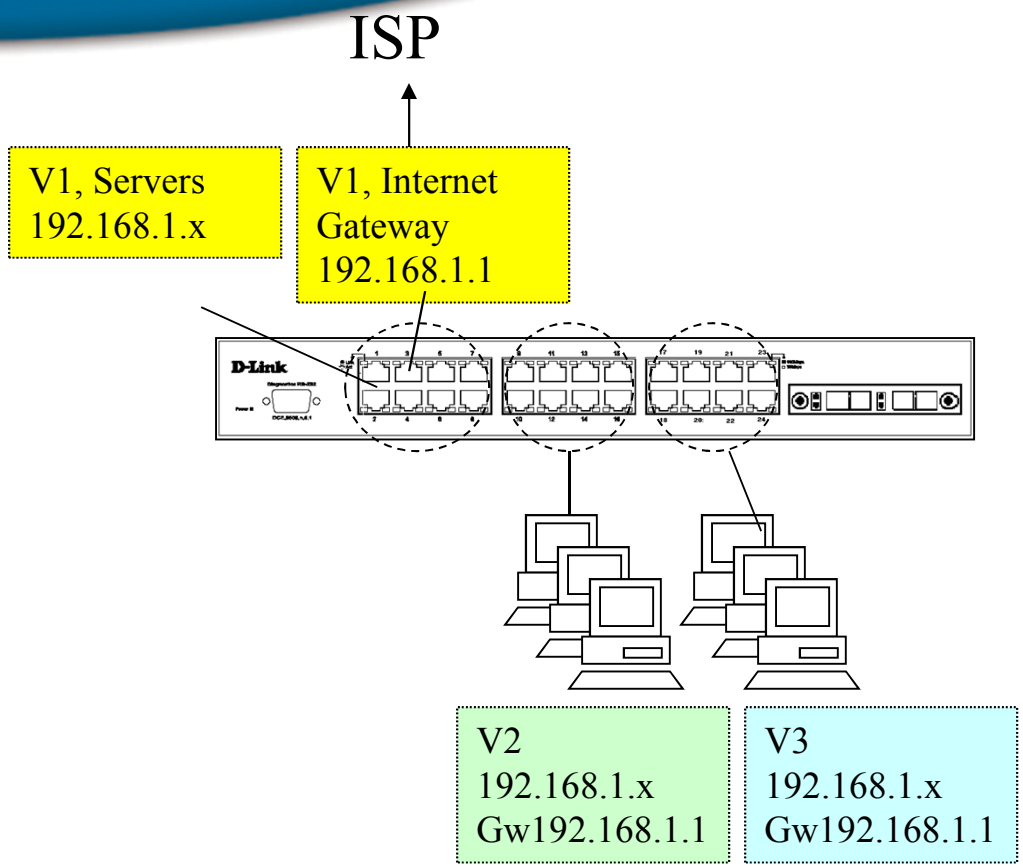
Asymmetric VLAN

- Need strong 802.1q VLAN knowledge
- VLAN membership can be across devices, and server can be anywhere.
- Special 802.1q support (overlapping untagged VLAN) is needed
- May not support IGMP snooping
- Max Vlan numbers limited to 4096.

Traffic Segmentation

- Simple, no VLAN knowledge is needed.
- VLAN membership cannot be across the devices
- IGMP snooping still works.
- Traffic Segmentation can be hierarchically. No Vlan number limitation.
- Shared servers must be at the “TOP” switch (when using hierarchically approach)

Example1: Asymmetric VLAN



V1: port 1-8, untagged
Shared Server(s) or Internet Gateway

V2: port 9-16, untagged
VLAN2 users (PC or hub/switch)

V3: port 17-24, untagged
VLAN3 users (PC or hub/switch)

Requirement:

1. V2 and V3 can access V1 for shared Server (with IPX, same network IP, AppleTalk, NetBEUI etc)
2. V2 and V3 can access Internet Gateway for Internet Access using same network IP.
3. No access between V2 and V3.

Example 1: Asymmetric VLAN

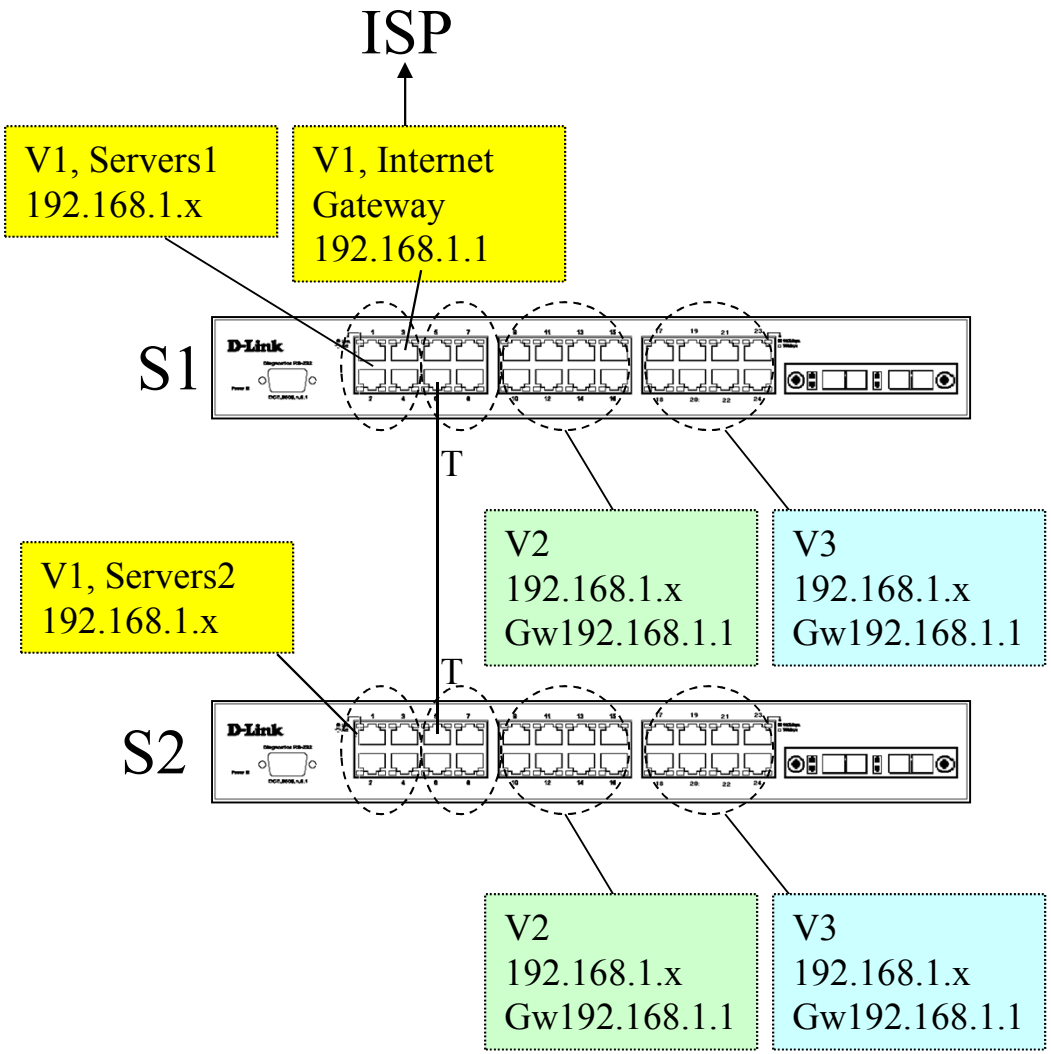
```
PVID and VLAN settings:
ports    1-8      9-16     17-24
================================
pvid     1..1     2..2     3..3
--------------------------------
VLANS
default  E..E     E..E     E..E
(V1)     U..U     U..U     U..U

V2       E..E     E..E     -..-
         U..U     U..U     -..-
V3       E..E     -..-     E..E
         U..U     -..-     U..U
```

```
enable asymmetric_vlan
create vlan v2 tag 2
create vlan v3 tag 3

config vlan v2 add untagged 1-16
config vlan v3 add untagged 1-8,17-24

config gvrp 1-8 pvid 1
config gvrp 9-16 pvid 2
config gvrp 17-24 pvid 3
save
```

Test:

1. V2 PC can access (ping) V1 servers and Internet Access is OK.
2 V3 PC can access (ping) V1 servers and Internet Access is OK.
3 V2 PC cannot see V3 PC, and V3 PC cannot see V2 PC.

Example 2: Asymmetric VLAN across two DGS-3426



V1: S1port1-4, S2port1-4, untagged
Shared Server(s) or Internet Gateway

S1port 5-8, S2 port 5-8 , tagged
for uplink/downlink to other switches

V2: S1port 9-16, S2port9-16,untagged
VLAN2 users (PC or hub/switch)

V3: S1port17-24, S2port17-24, untagged
VLAN3 users (PC or hub/switch)

Requirement:

1. V2 and V3 can access V1 for shared Server (with IPX, IP, AppleTalk, etc) or Internet Gateway
2. V2 and V3 cannot see each other

Example 2: Asymmetric VLAN across two DGS-3426

S1 settings

```
ports    1-4      5-8      9-16     17-24
=======================================
pvid     1..1     1..1     2..2     3..3
---------------------------------------
VLANs
default  E..E     E..E     E..E     E..E
(V1)     U..U     T..T     U..U     U..U

V2       E..E     E..E     E..E     -..-
         U..U     T..T     U..U     -..-

V3       E..E     E..E     -..-     E..E
         U..U     T..T     -..-     U..U
```

```
enable asymmetric_vlan
create vlan v2 tag 2
create vlan v3 tag 3

config vlan default delete 5-8
config vlan default add tagged 5-8
config vlan v2 add untagged 1-4,9-16
config vlan v2 add tagged 5-8
config vlan v3 add untagged 1-4,17-24
config vlan v3 add tagged 5-8

config gvrp 1-8 pvid 1
config gvrp 9-16 pvid 2
config gvrp 17-24 pvid 3
save
```

Example 2: Asymmetric VLAN across two DGS-3426

S2 settings

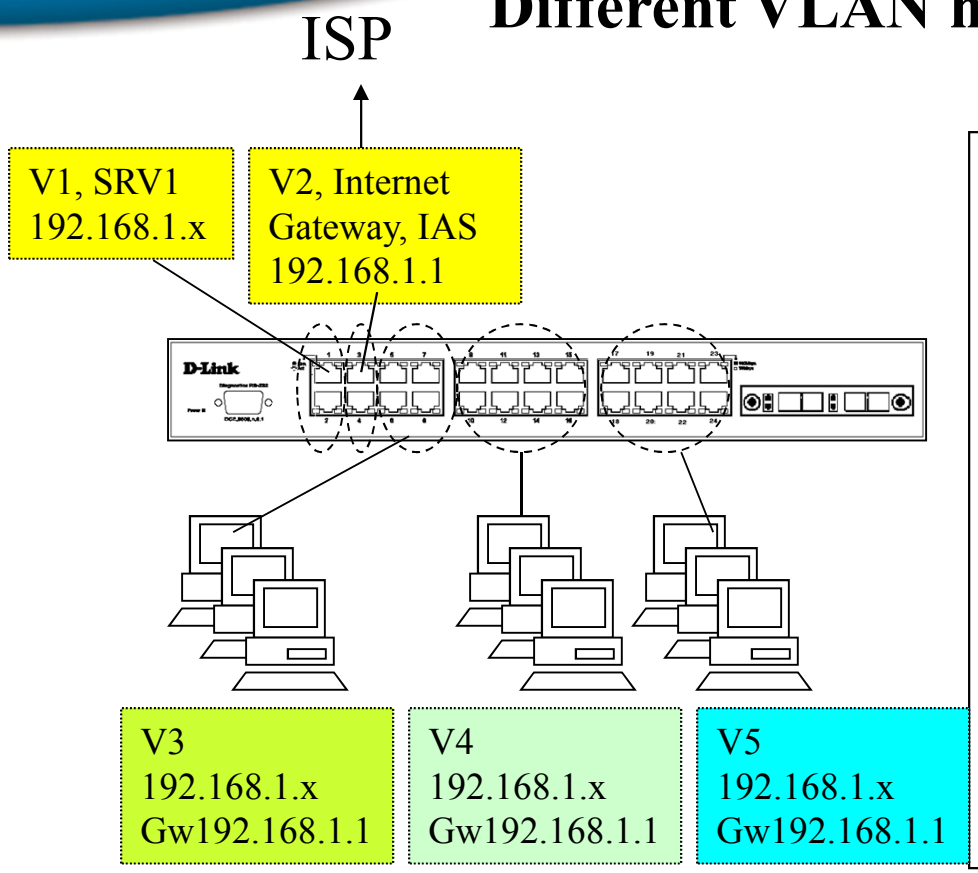
```
ports    1-4      5-8      9-16     17-24
=======================================
pvid     1..1     1..1     2..2     3..3
---------------------------------------
default  E..E     E..E     E..E     E..E
(V1)     U..U     T..T     U..U     U..U

V2       E..E     E..E     E..E     -..-
         U..U     T..T     U..U     -..-

V3       E..E     E..E     -..-     E..E
         U..U     T..T     -..-     U..U
```

```
enable asymmetric_vlan
create vlan v2 tag 2
create vlan v3 tag 3

config vlan default delete 5-8
config vlan default add tagged 5-8
config vlan v2 add untagged 1-4,9-16
config vlan v2 add tagged 5-8
config vlan v3 add untagged 1-4,17-24
config vlan v3 add tagged 5-8

config gvrp 1-8 pvid 1
config gvrp 9-16 pvid 2
config gvrp 17-24 pvid 3
save
```

Test:

1. V2 PC (at S1 or S2) can access (ping) V2 PC (at S1 or S2).
2. V3 PC (at S1 or S2) can access (ping) V3 PC (at S1 or S2). ➔ Members across switch is OK.
3. V2 PC (at S1 or S2) can access V1 servers and Internet Access is OK.
4. V3 PC (at S1 or S2) can access V1 servers and Internet Access is OK. ➔ Shared VLAN is OK.
5. V2 PC (at S1 or S2) cannot see V3 PC (at S1 or S2),
6. V3 PC (at S1 or S2) cannot see V2 PC (at S1 or S2).➔ No access between VLANs

Example 3: Asymmetric VLAN
Different VLAN has different server access right



Standalone

SRV1: ports 1,2
Internet Access: ports 3,4
VLAN3: 5-8
VLAN4: 9-16
VLAN5: 17-24

Requirements:

- V3 can access V1 SRV1, but CANNOT access V2 for Internet Access.
- V4 can access V1 servers, and V2 for Internet Access.
- V5 can access V2 for Internet access, but CANNOT access V1 Servers.
- V3, V4, V5 no access in between.

Example 3: Asymmetric VLAN
Different VLAN has different server access right

PVID and VLAN settings:

VLAN	V1	V2	V3	V4	V5
ports	1-2	3-4	5-8	9-16	17-24
pvid	1..1	2..2	3..3	4..4	5..5
default	E..E	E..E	E..E	E..E	---
(V1)	U..U	U..U	U..U	U..U	---
V2	E..E	E..E	---	E..E	E..E
	U..U	U..U	---	U..U	U..U
V3	E..E	---	E..E	---	---
	U..U	---	U..U	---	---
V4	E..E	E..E	---	E..E	---
	U..U	U..U	---	U..U	---
V5	---	E..E	---	---	E..E
	---	U..U	---	---	U..U

Example 3: Asymmetric VLAN
Different VLAN has different server access right

Configuration

```
enable asymmetric_vlan
# default vlan is created by default
create vlan v2 tag 2
create vlan v3 tag 3
create vlan v4 tag 4
create vlan v5 tag 5

config vlan default delete 17-24
config vlan v2 add untagged 1-4,9-24
config vlan v3 add untagged 1-2,5-8
config vlan v4 add untagged 1-4, 9-16
config vlan v5 add untagged 3-4, 17-24

config gvrp 1-2 pvid 1
config gvrp 3-4 pvid 2
config gvrp 5-8 pvid 3
config gvrp 9-16 pvid 4
config gvrp 17-24 pvid 5

save
```

Test

1. V3 user can access V1 server only, but cannot access V2, and other Vlans (V4, V5)

2. V4 user can access V1 and V2 (Internet Access), but cannot access V4 and V5.

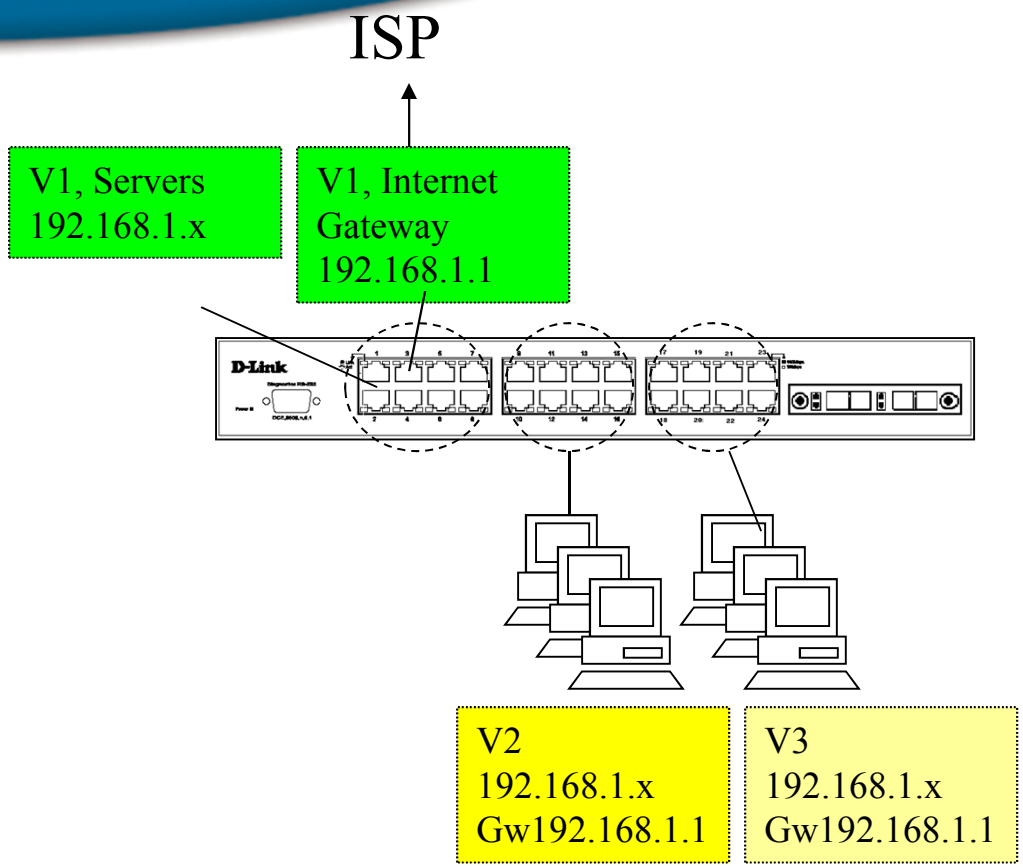
3. V5 user can access V2 (Internet Access), but cannot access V1, and

Asymmetric VLAN Limitation

The IGMP Snooping cannot be supported Asymmetric VLANs.

Resolution: L3 Switch + ACL + Multicast routing + IGMP snooping

Traffic Segmentation



V1: port 1-8
Shared Server(s) or Internet Gateway

V2: port 9-16
VLAN2 users (PC or hub/switch)

V3: port 17-24
VLAN3 users (PC or hub/switch)

Requirement:

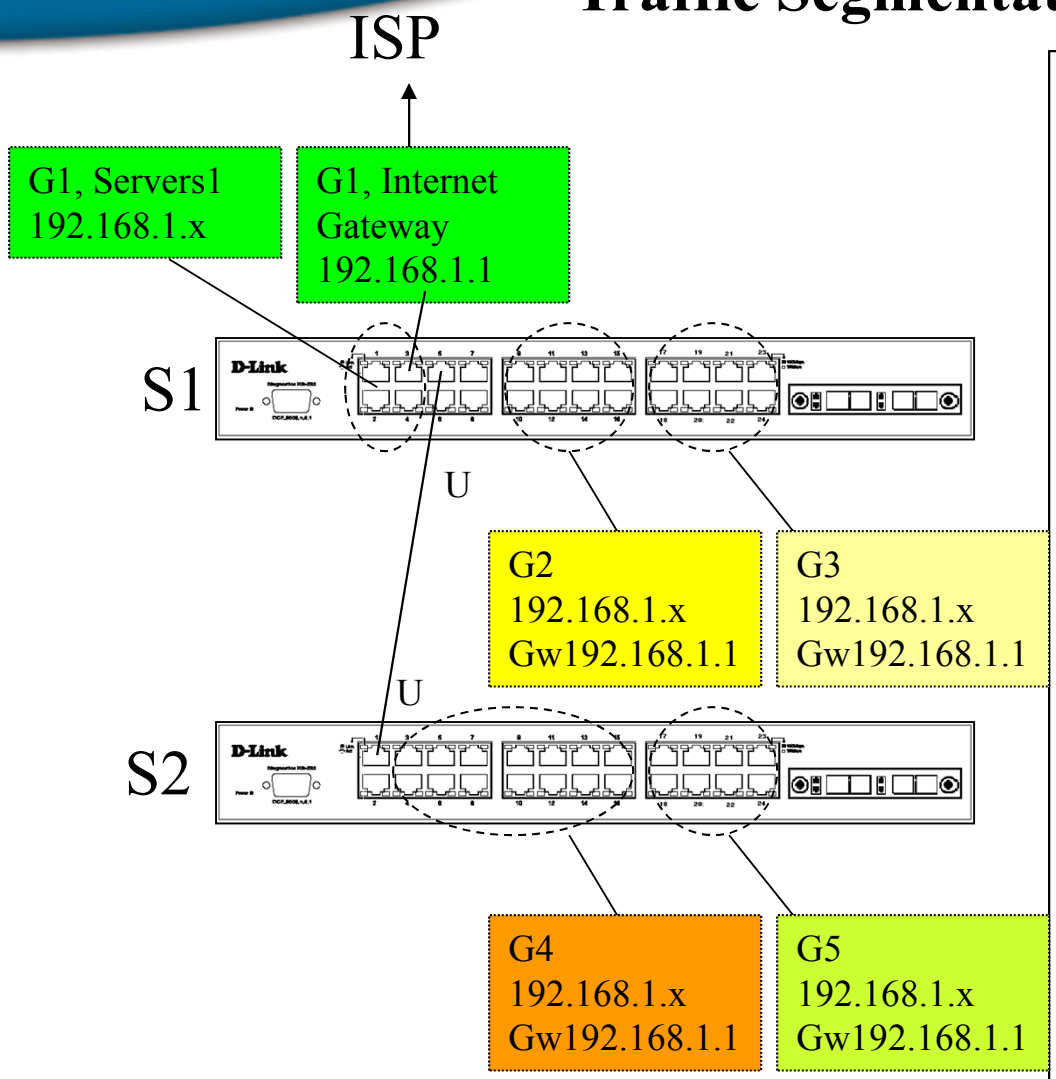
1. V2 and V3 can access V1 for shared Server (with IPX, same network IP, AppleTalk, NetBEUI etc)
2. V2 and V3 can access Internet Gateway for Internet Access using same network IP.
3. No access between V2 and V3.

D-Link
Building Networks for People

DGS-3426 Configuration

```
config traffic_segmentation 1-24 forwarding_list 1-24
config traffic_segmentation  9-16 forwarding_list 1-16
config traffic_segmentation 17-24 forwarding_list 1-8,17-24
```

Traffic Segmentation two level hierarchy



S1port1-4: G1, untagged
Shared Server(s) or Internet Gateway

S1port 5-8, S2 port 1-2 , untagged
for uplink/downlink to other switches

S1port 9-16: G2, untagged
VLAN2 users (PC or hub/switch)

S1port17-24: G3, untagged
group3 users (PC or hub/switch)

S2Port1: uplink port

S2port 3-16: G4, untagged
Group 4 users (PC or hub/switch)

S2port 17-24: G5
Group 5 users (PC or hub/Switch)

Requirement:

1. All groups (G2 to G5) can access shared Server (with IPX, IP, AppleTalk, etc) or Internet Gateway at G1.
2. G2, G3, G4, G5 no access in between.

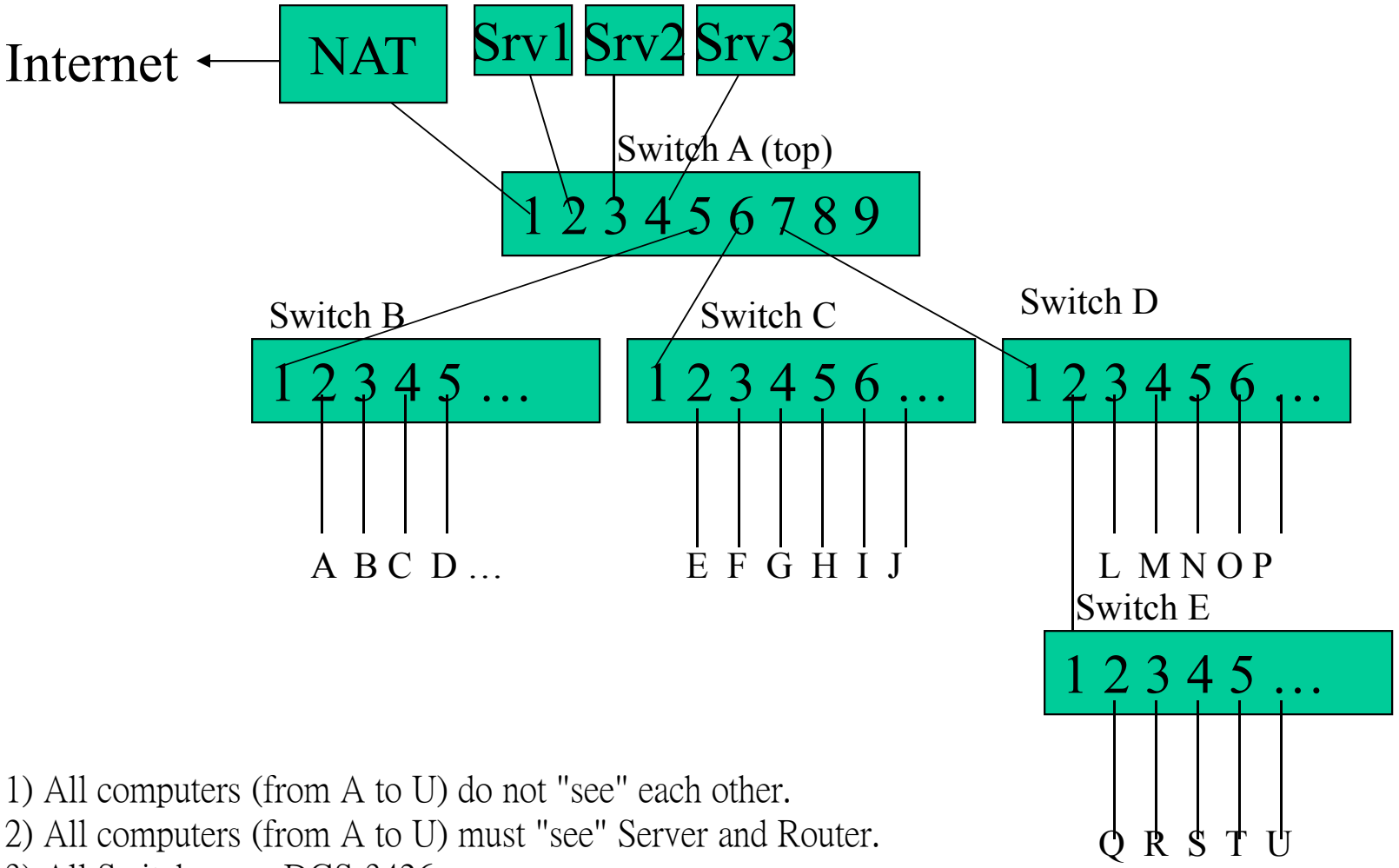
S1 configuration (Top level switch)

```
config traffic_segmentation 1-4 forwarding_list 1-24
config traffic_segmentation  5 forwarding_list 1-5
config traffic_segmentation  9-16 forwarding_list 1-4, 9-16
config traffic_segmentation  17-24 forwarding_list 1-4, 17-24
```

S2 Configuration (lower level switch)

```
config traffic_segmentation 1 forwarding_list 1-24
config traffic_segmentation  2-16 forwarding_list 1-16
config traffic_segmentation 17-24 forwarding_list 1,17-24
```

Hierarchical Traffic Segmentation for Port-isolation



1) All computers (from A to U) do not "see" each other.
2) All computers (from A to U) must "see" Server and Router.
3) All Switches are DGS-3426.

4) Same IP subnet IP address between computers and server/NAT.

Configuration

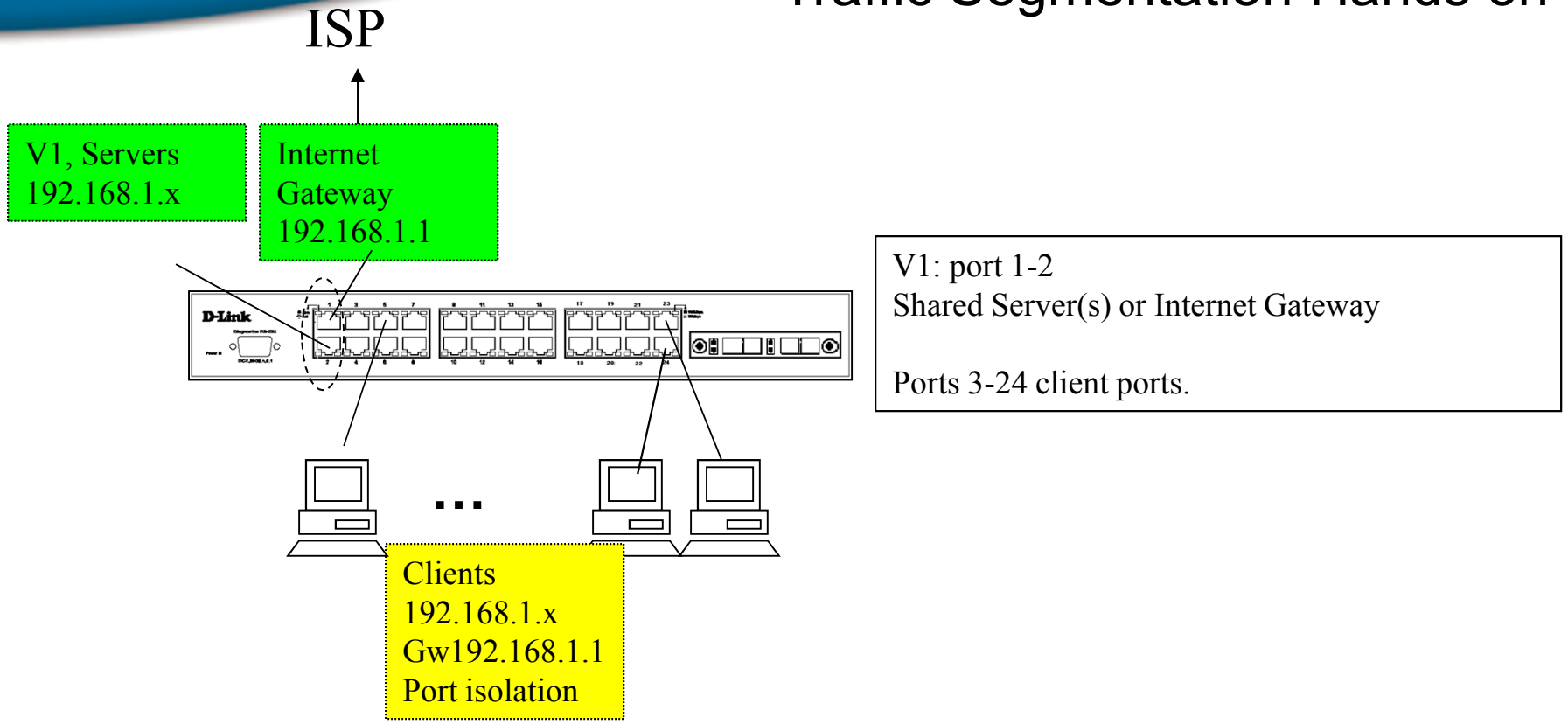
Switch A (top)

```
config traffic_segmentation 1-4 forwarding_list 1-26
config traffic_segmentation  5 forwarding_list 1-5
config traffic_segmentation  6 forwarding_list 1-4,6
config traffic_segmentation  7 forwarding_list 1-4,7
(repeat for other downlink ports)
```

Switch B, C, D, E,… (others)

```
config traffic_segmentation 1 forwarding_list 1-26
config traffic_segmentation 2-24 forwarding_list 1
```

Traffic Segmentation Hands on



Configure DGS-3426 using “traffic Segmentation” to meet the Requirements:

1. All clients can access the server connecting to Port 1 and port2.
2. No Access between client ports (3-24).

D-Link
Building Networks for People

THANK YOU