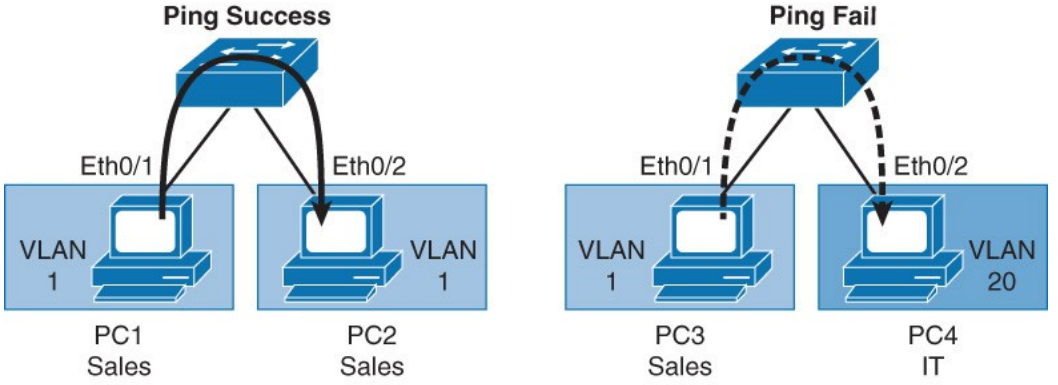
Campus Networks:
VLAN Redux: PVLANs
NET3011 – 17W

The Problem of Scaling

- Ch 3 said VLANs are a solution to flat networks:
  - VLANs isolate traffic and thus provide a logical broadcast domain [and (a limited form of) security]
  - Ports in same VLAN share broadcasts; ports in different VLANs do not
- VLANs, however, have lots of extra overhead: e.g. L2 design, subnetting (1 per VLAN), management, protocols (DTP, VTP, STP)
- Can we get the benefits without the overhead?



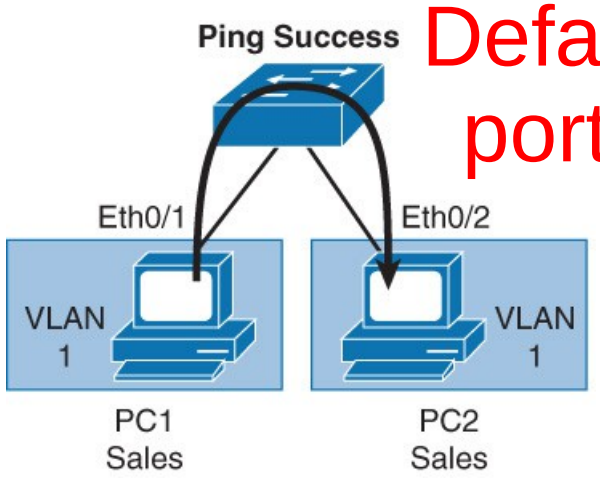
- VLAN is an independent LAN network.
- VLAN = broadcast domain.
- VLAN maps to logical network (subnet).
- VLANs provide segmentation, security, and network flexibility.

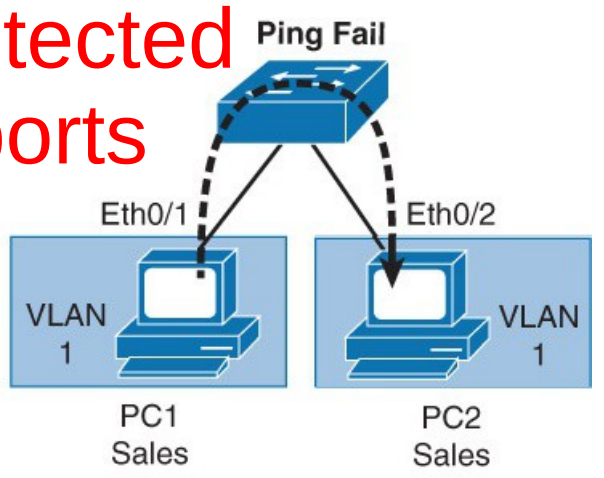
Option 1: Protected Ports

- Cisco (and other vendors) provide a mechanism to isolate individual hosts within the same VLAN:

```
Sw(config-if)#  switchport protected
```

- Also referred to as PVLAN Edge ports
- Behaviour is explained by one simple rule: "protected ports can **NOT** communicate (directly)" … no broadcast, no unicast, no multicast, nothing!



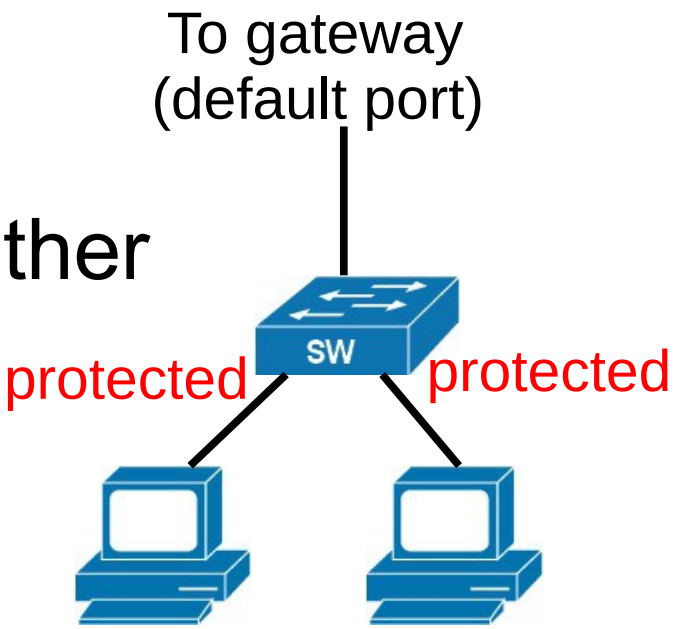


Protected Ports – Basics

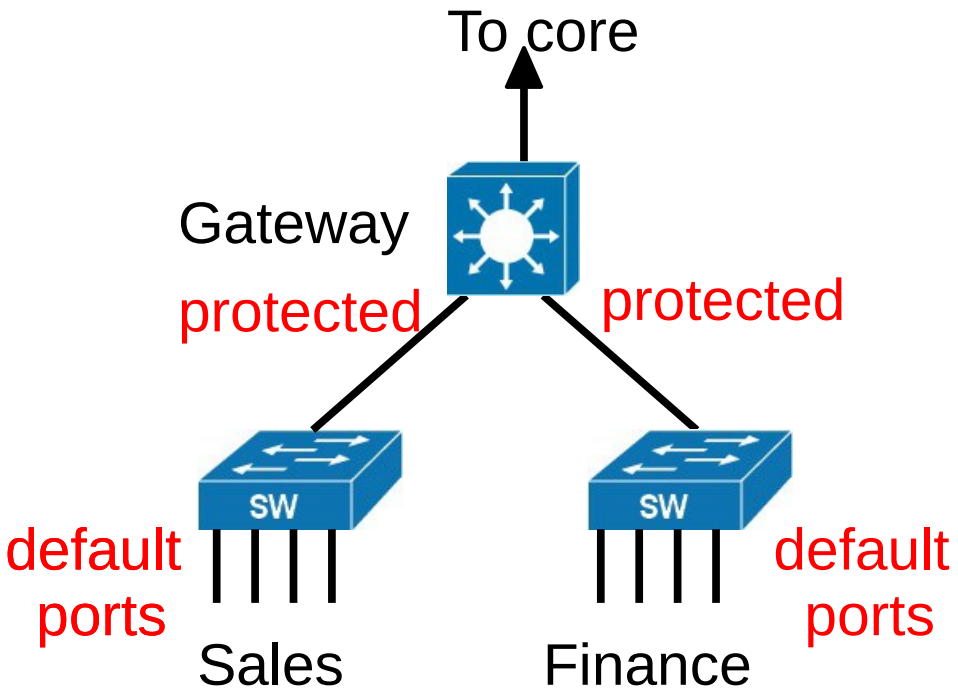
- Extremely simple config: exactly & only 1 line
- Extremely simple operation:
  - no direct L2 communication between protected ports
  - protected ports may communicate via L3 (routing)
  - full communication with non-protected (default) ports
- Provides multiple benefits:
  - limited broadcast domain for protected ports
  - security (isolation) between protected ports
  - eliminates needs for VLANS (DTP, VTP, STP)
  - option for a *single subnet*
  - excellent option for wireless / WAP networks
  - still able to choose how far down to push L3
  - equivalent to solutions available & used by ISPs

Protected Port examples

- Isolate all users (eg. students)
  - users can't interfere with each other
  - users have access to GW
  - can create DMZ "safe-zone"



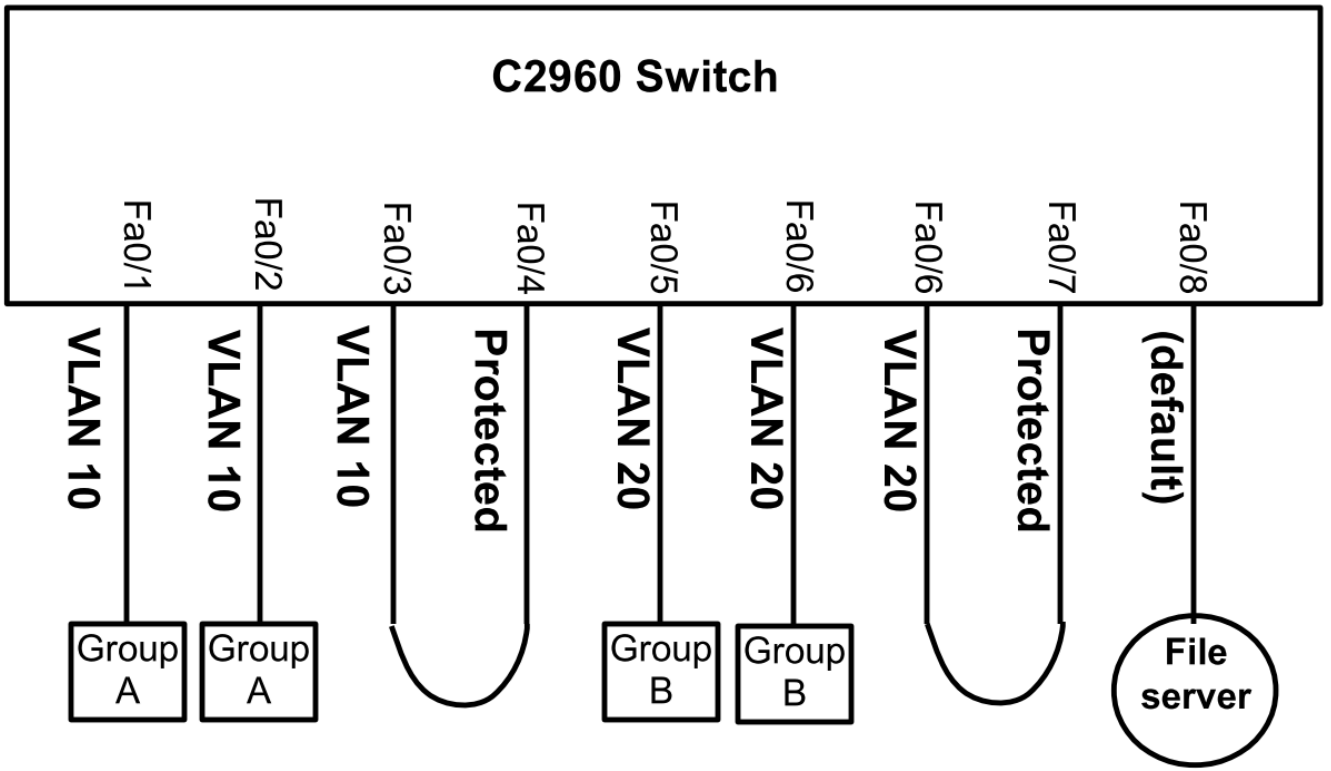
- Communities of users



- users on <u>each</u> access SW can communicate
- all users can access common resource
- each group is isolated

Single-switch Protected Port soln's

- Multiple groups all accessing common resources
  - Use a (local) VLAN for each community
  - Join VLANs to protected ports
  - Connect resources (server, GW) to default ports
  - (Need to deal with unwanted STP BPDUs)

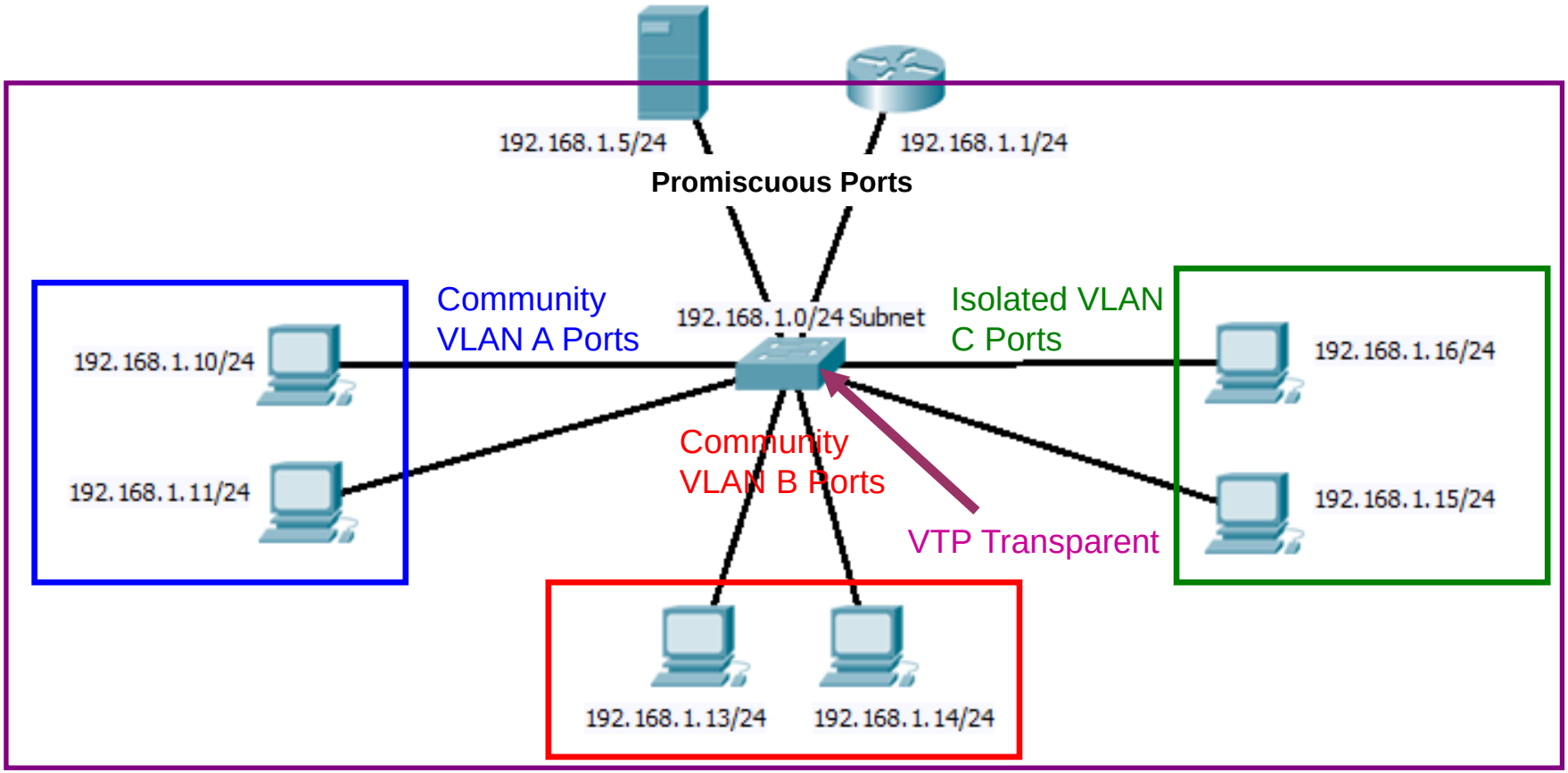


Option 2: Private VLANs – Basics

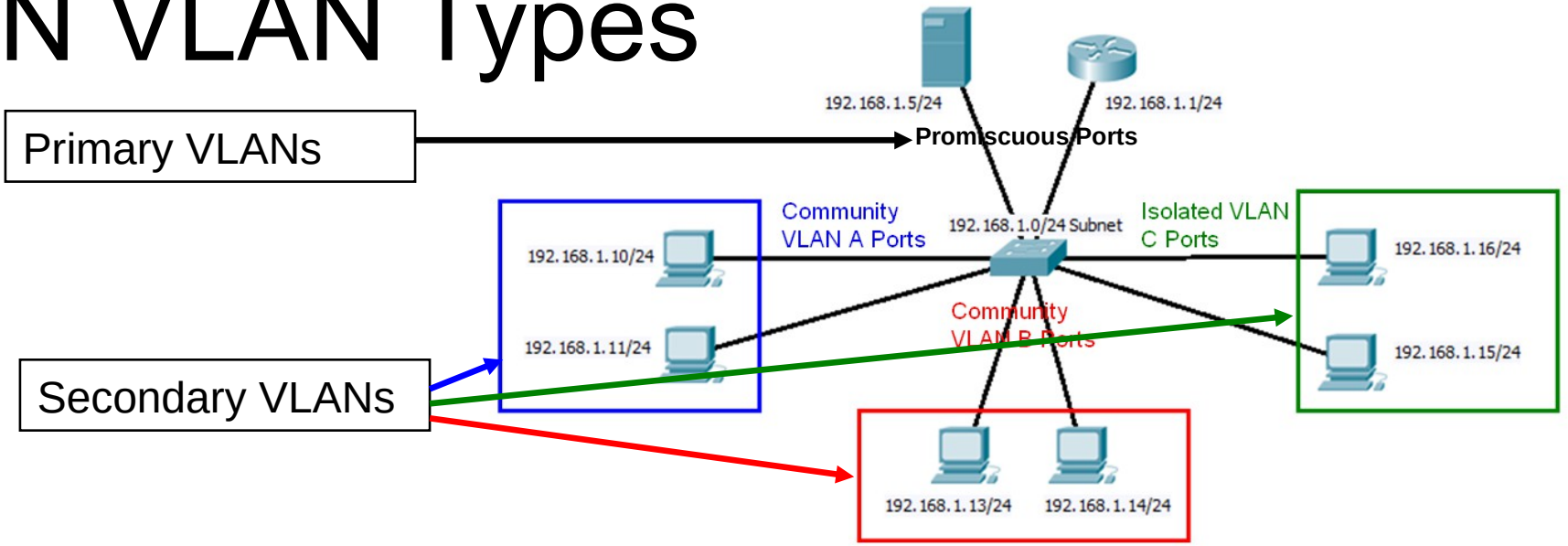
- Design with three categories of connectivity:
  - **isolated**, individual host ports
  - **community** ports with sharing only by members
  - **promiscuous** ports for common resources
- PVLAN comparison with Protected ports:
  - design is simpler
  - multiple switches are never *required*
  - can easily span multiple switches if desired
  - configuration is *waaaay* longer and much more prone to mistakes
  - propagation of PVLANs is supported in VTP v3, otherwise must use Transparent mode and configure each switch individually

PVLAN Topology

- Scenario showing all three types of PVLAN ports



PVLAN VLAN Types

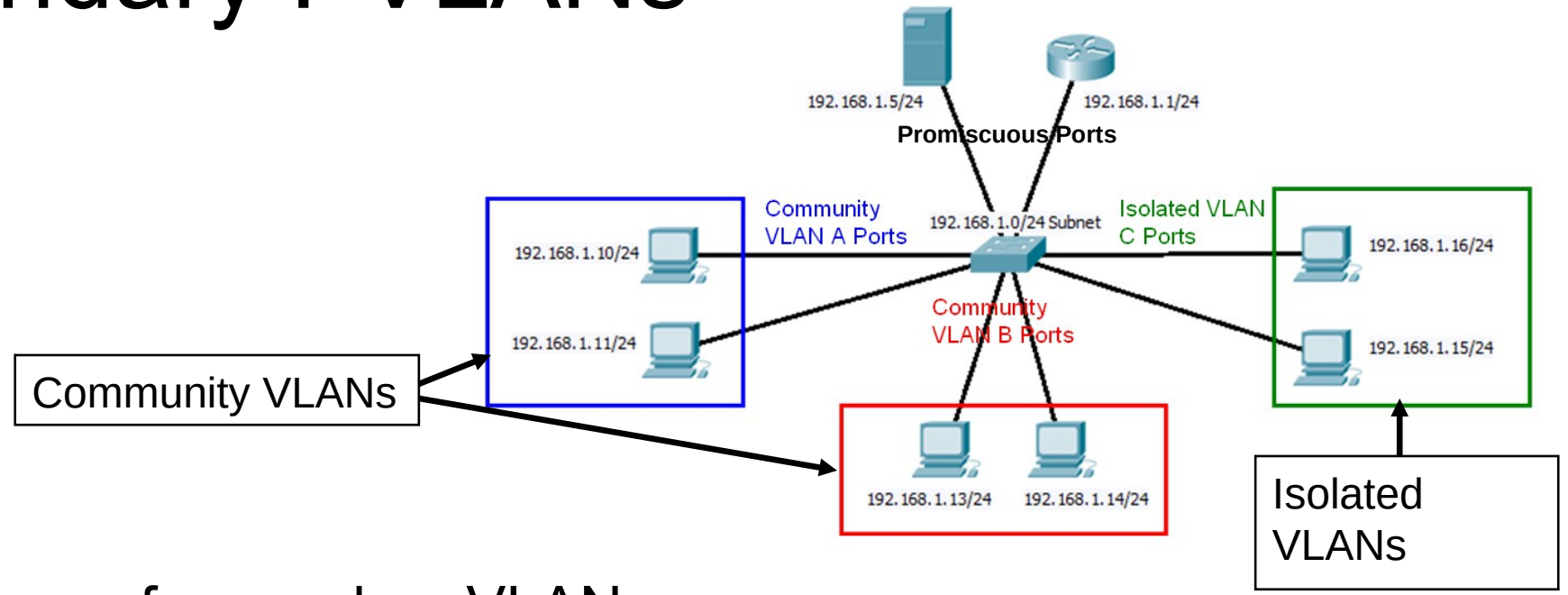


PVLANs consist of two types of supporting VLANs:

- **Primary VLAN**
  - High-level VLAN; only one type: **promiscuous**

- **Secondary VLAN**
  - Child to a Primary
  - Non-promiscuous end devices connect to a secondary VLAN
  - Can have many secondary VLANs; all belong to one subnet

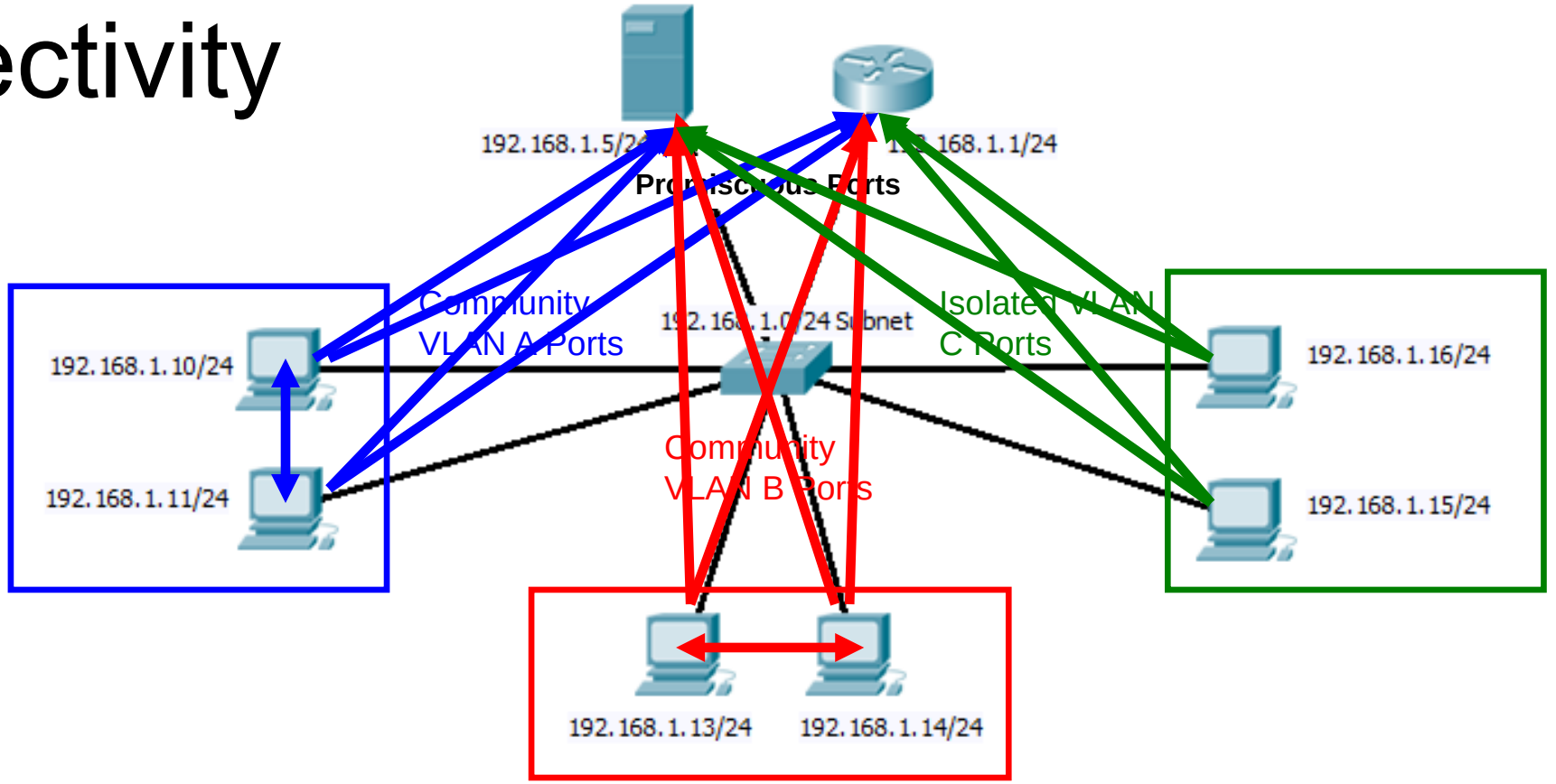
Secondary PVLANs



Two types of secondary VLANs:

- **Community VLANs**
  - These ports communicate with other ports in the same community and promiscuous ports.
- **Isolated VLANs**
  - These ports can only communicate with promiscuous ports.
  - Maximum of 1 isolated VLAN associated with a Primary VLAN

Connectivity



- Community VLAN ports communicate with other ports in the same community and promiscuous ports.
  - What devices can Community VLAN A PCs communicate with?
  - What devices can Community VLAN B PCs communicate with?
- Isolated VLANs ports can only communicate with promiscuous ports
  - What devices can Isolated VLAN C PCs communicate with?

Implementing PVLANs

- not available on 29xx (L2) or 3550 (older) devices
- pVLAN implementation and configuration commands (and options) vary between platforms
  - download the command reference and/or configuration guide associated with your platform(s) from cisco.com
- when a command parameter is a list of VLAN IDs:
  - a single value can be specified (e.g. 100)
  - multiple values separated by commas, with some platforms disallowing spaces (e.g. 100,101,104)
  - range can be specified using a hyphen (e.g. 100-105)

Configuring pVLANs – Steps

Step 1. Set VTP mode to transparent (assume VTP v2 is in use)

Step 2. Create the secondary pVLANs.

Step 3. Create the primary pVLAN.

Step 4. Associate the secondary pVLAN with the primary pVLAN. Only one isolated pVLAN can be mapped to a primary pVLAN, but more than one community pVLAN can be mapped to a primary pVLAN.

Step 5. Map the promiscuous ports to the secondary pVLANs with which they will communicate.

Step 6. Configure interfaces as promiscuous ports.

Step 7. Associate the isolated ports and community ports with their corresponding primary-secondary pVLAN pair.

Step 8. Configure interfaces as isolated or community ports.

Step 9. Create all primary and secondary pVLANs on intermediate switches that are traversed, even if they contain no pVLAN ports.

Configuring PVLANs–Cmd Summary

- **Steps 2, 3: Create private VLANs (secondaries & primary)**

```
Switch(config)# vlan pvlan-id
Switch(config-vlan)# private-vlan {community | isolated | primary}
```

- **Step 4: Associate primary VLAN to all secondary VLANs**

```
Sw(config)# vlan primary-vlan-id
Sw(config-vlan)# private-vlan association [add | remove] secondary-vlan-list
```

- **Start configuration of switch ports where hosts will be connected; ensure L2 mode**

```
Switch(config)# interface type slot/port
Switch(config-if)# switchport
```

if port defaults to L3 operation

Step 5: for primary VLAN promiscuous ports, associate the list of reachable secondary VLANs

```
Switch(config-if)# switchport private-vlan mapping primary-vlan-id
                                                  [add | remove] secdry-vlan-list
```

Step 7: for secondary VLAN ports, associate the primary VLAN

```
Switch(config-if)# switchport private-vlan host-association
                                                  primary-vlan-id secondary-vlan-id
```

- **Steps 6, 8: Activate the switchport operating mode as secondary or primary**

```
Switch(config-if)# switchport mode private-vlan {host | promiscuous}
```

- **(Extra) If L3 switching, map primary VLAN SVI to all secondary VLANs**

```
Switch(config)# interface vlan primary-vlan-id
Switch(config-if)# private-vlan mapping [add | remove] secondary-vlan-list
```

Verifying pVLAN Configuration

- The two most useful commands for this are:

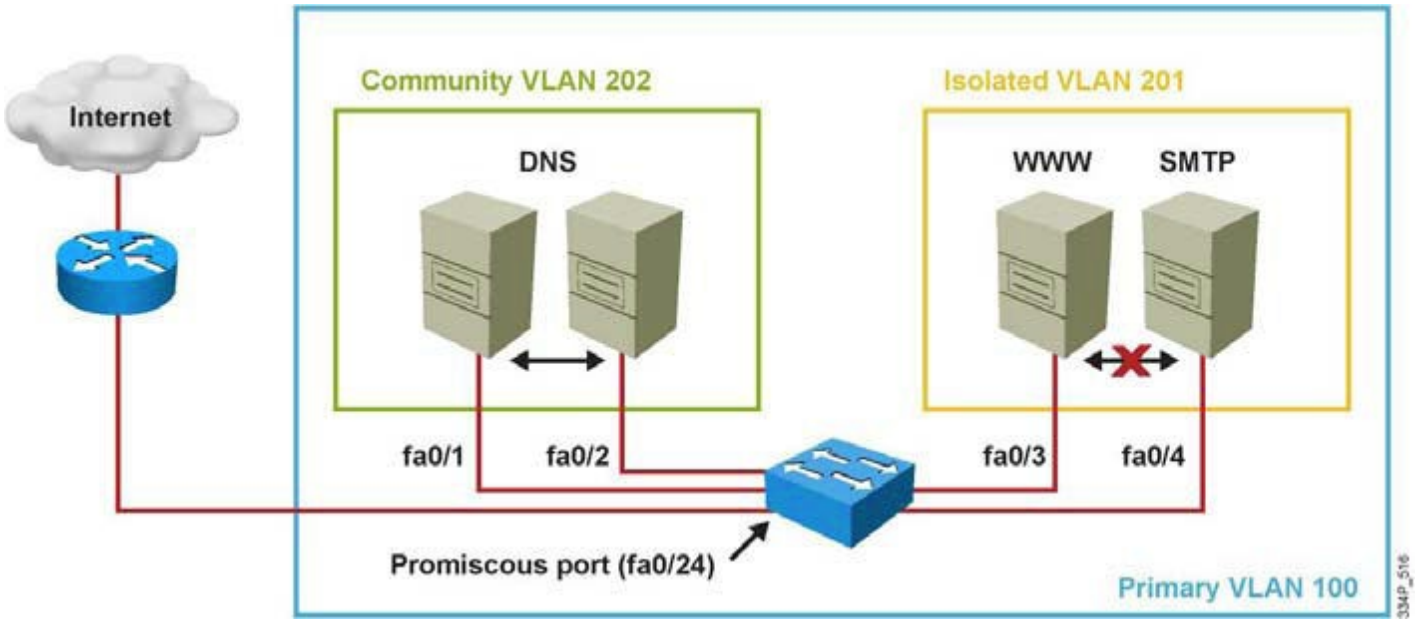
  show vlan private-vlan

  show interfaces *interface* **switchport**

```
Switch# show vlan private-vlan
Primary   Secondary   Type              Interfaces
-------   ---------   --------------    -----------------
100       200          community
100       300          isolated          Fa5/2

Switch# show interfaces FastEthernet 5/2 switchport
Name: Fa5/2
Switchport: Enabled
Administrative Mode: private-vlan host
Operational Mode: down
Administrative Trunking Encapsulation: negotiate
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Administrative private-vlan host-association: 100 (VLAN0100) 300 (VLAN0300)
Administrative private-vlan mapping: none
Operational private-vlan: none
[... output omitted ...]
```

Single-switch PVLAN



- A corporate DMZ contains two DNS servers, one web server and one SMTP server. All servers and their connecting router are in the same subnet.
- DNS servers are redundant copies, so they need to communicate with each other to update their entries and to the Internet. In addition to that, they also need to communicate with the Internet.
- The Web Server and the SMTP server needs to communicate with the Internet, but for security purposes, the SMTP server should not be reachable from the Web or the DNS servers. The web server needs to be accessible from the Internet but not from the SMTP server.

Single-switch PVLAN Configuration

```
Switch(config)# vtp mode transparent
```
Step 1: VTP transparent needed for pVLANs

```
Switch(config)# vlan 201
Switch(config-vlan)# private-vlan isolated
Switch(config)# vlan 202
Switch(config-vlan)# private-vlan community
```
Step 2: configure secondary pVLANs

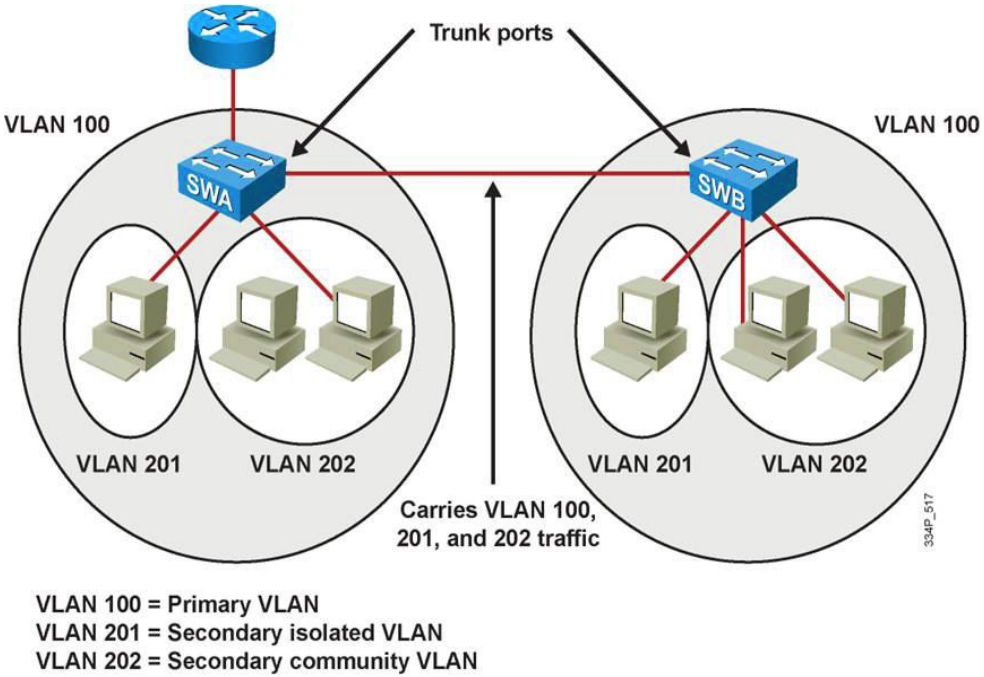
```
Switch(config-vlan)# vlan 100
Switch(config-vlan)# private-vlan primary
Switch(config-vlan)# private-vlan association 201,202
```
Step 3: configure primary pVLAN, associating secondaries

```
Switch(config-vlan)# interface fastethernet 0/24
Switch(config-if)# switchport private-vlan mapping 100 201,202
Switch(config-if)# switchport mode private-vlan promiscuous
```
promiscuous port on VLAN 100

```
Switch(config-if)# interface range fastethernet 0/3 - 4
Switch(config-if)# switchport private-vlan host-association 100 201
Switch(config-if)# switchport mode private-vlan host
```
isolated ports on VLAN 201

```
Switch(config-if)# interface range fastethernet 0/1 - 2
Switch(config-if)# switchport private-vlan host-association 100 202
Switch(config-if)# switchport mode private-vlan host
```
community ports on VLAN 202

Multi-switch PVLAN



- A standard trunk port carries traffic for primary and secondary VLANs to a neighbouring switch just like any other VLAN. This is NOT a pVLAN trunk! (next)
- Frames on a trunk originating from a pVLAN host are tagged with the VLAN ID on which that host's switchport is configured (whether primary or sec)
  - For example, from the rightmost host on SWB a frame sent to the router will be tagged with VLAN ID 202 across the trunk link, but the router's reply will be tagged with VLAN ID 100.
- A feature of pVLANs across multiple switches is that traffic from an isolated port in one switch does not reach an isolated port on another switch.
- Configure pVLANs on all switches along the path, including devices that have no pVLAN ports – this maintains the security of your pVLAN configuration.
  - But of course, do NOT associate ports to those VLAN IDs already configured as pVLANs!
  - Best practice: all switches having pVLAN ports are contiguous, connected by trunks.

PVLAN config: Too confusing?

- If you're stymied by the PVLAN config, you can substitute some brain power for configuration skill and go back to simpler protected ports.
- Here's an example showing all three port types