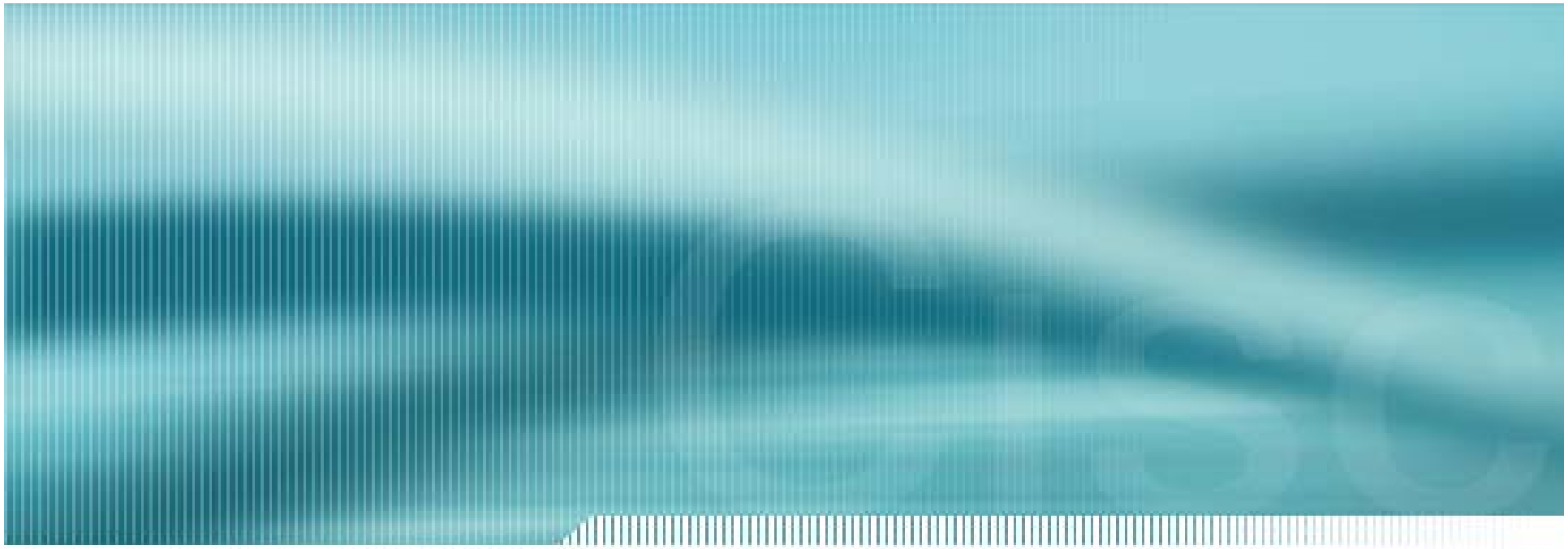


Inter-VLAN Routing

Malin Bornhager

Halmstad University

Objectives

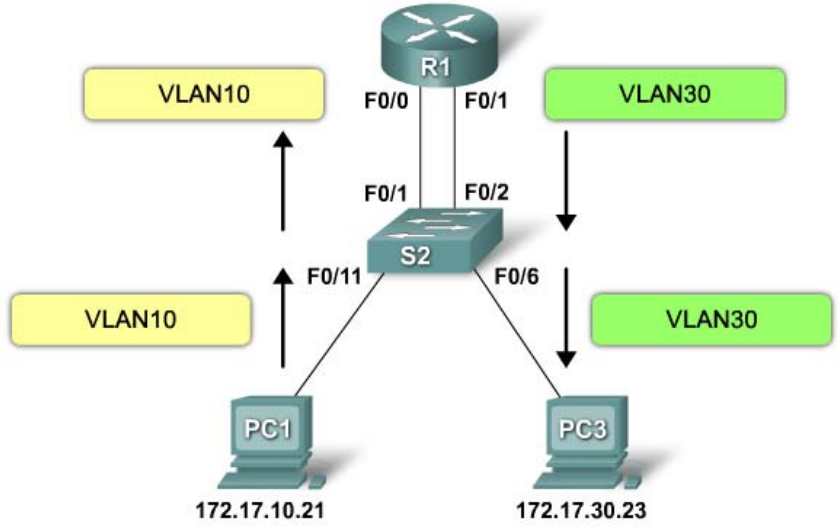
- **Inter-VLAN Routing**
- **Router-on-a-Stick**
- **Subinterface configuration**
- **Switch Security**

VLANs

- VLANs can be used to segment the network
- Reduce the size of the broadcast domain
  - Each VLAN is a unique broadcast domain
  - Different IP subnets
- No communication between VLANs
- Inter-VLAN routing is the process of forwarding network traffic from one VLAN to another VLAN using a router

Inter-VLAN Routing

- **The router interfaces can be connected to separate VLANs**
- **One subnet on each interface**
  - **Routing between subnetworks**

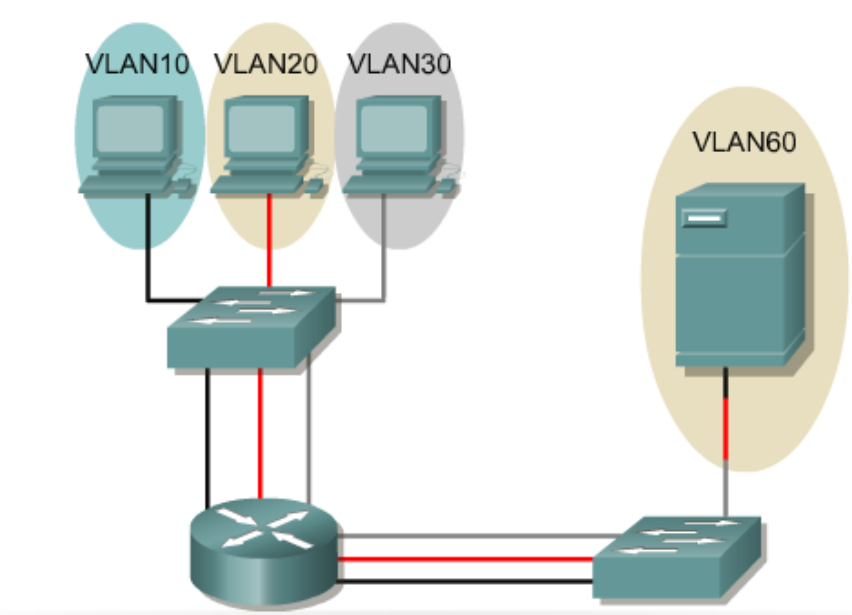


Router-based Inter-VLAN routing is a process for forwarding network traffic from one VLAN to another VLAN using a router.

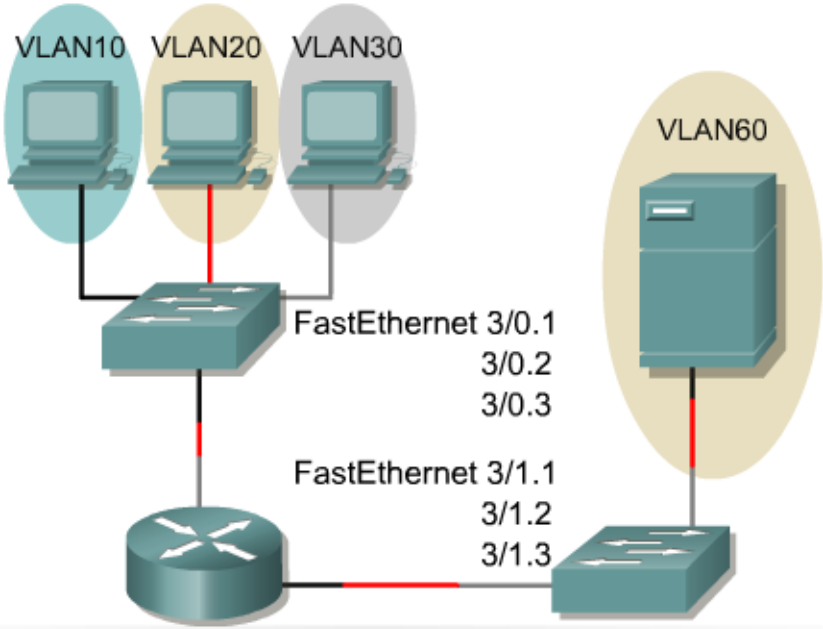
Inter-VLAN Routing

- Traditionally, LAN routing has used routers with multiple physical interfaces
- Each interface needed to be connected to a separate network
  - Configured for a different subnet
- Each router interface is connected to a switch port, associated with a specific VLAN
- The router can accept traffic from the VLAN associated with the switch interface it is connected to, and route the traffic to other VLANs

Physical and Logical Interfaces



The router supports one VLAN per interface.



A single ISL link can support multiple VLANs.

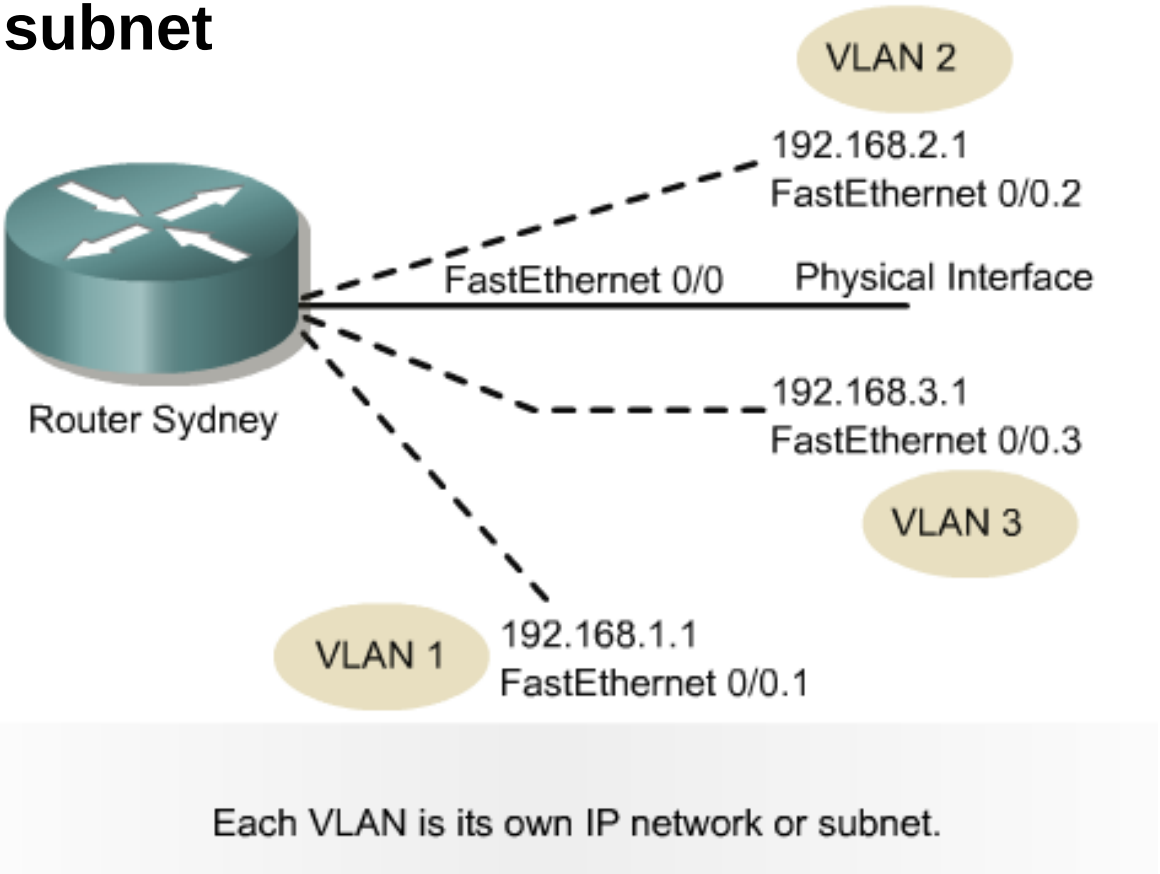
- **Router interfaces can be configured as trunk links**
- **Multiple VLANs can be supported on one physical link**

Router-on-a-Stick

- A type of router configuration in which a single router interface routes traffic between multiple VLANs
- The connection between the switch and the router is a single trunk link
- The router accept VLAN tagged traffic on the trunk interface
- Route traffic between the different VLANs

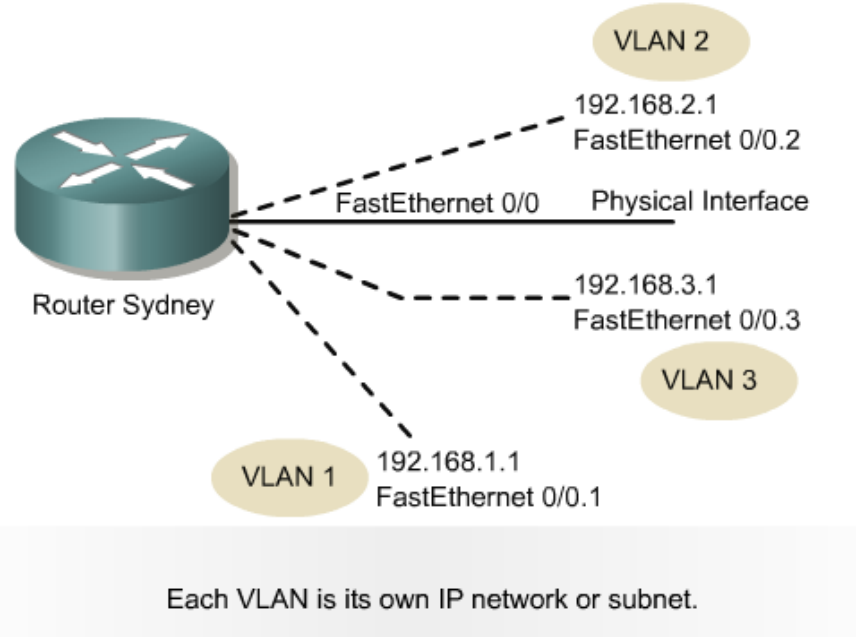
Router-on-a-Stick

- **The physical interface is divided into multiple subinterfaces**
- **Each subinterface is associated with one VLAN and one IP subnet**



Router-on-a-Stick

- **By configuring IP addresses on the interfaces, the router can be used as a gateway to access devices connected to the other VLANs**
- **If the destination address is on a remote network (another VLAN), the routing table is used to forward the data to the correct destination**



Configuring Inter-VLAN Routing

Subinterface Configuration

```
R1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#interface f0/0.10
R1(config-subif)#encapsulation dot1q 10
R1(config-subif)#ip address 172.17.10.1 255.255.255.0
R1(config-subif)#interface f0/0.30
R1(config-subif)#encapsulation dot1q 30
R1(config-subif)#ip address 172.17.30.1 255.255.255.0
R1(config-subif)#interface f0/0
R1(config-if)#no shutdown
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up
%LINK-5-CHANGED: Interface FastEthernet0/0.10, changed state to up
%LINK-5-CHANGED: Interface FastEthernet0/0.30, changed state to up
R1(config-if)#end
R1#
```

Configuring inter-VLAN Routing (cont.)

Subinterface Configuration

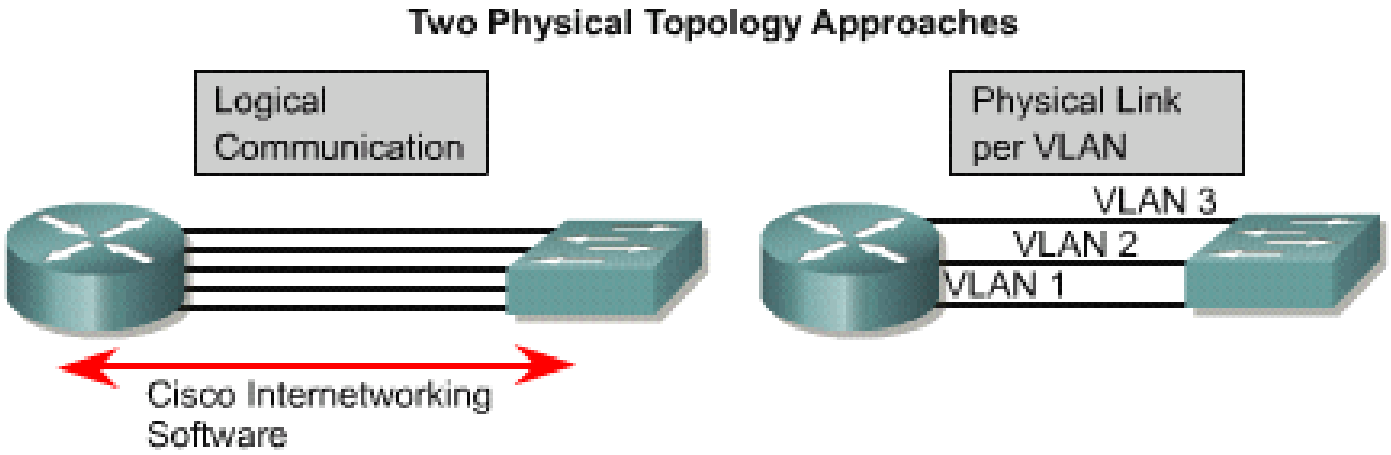
```
R1#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B -
BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS
inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

     172.17.0.0/24 is subnetted, 2 subnets
C       172.17.10.0 is directly connected, FastEthernet0/0.10
C       172.17.30.0 is directly connected, FastEthernet0/0.30
```

Routing Table for this subinterface configuration

Communication between VLANs



Using Layer 3 routers to link VLANs provides the following benefits:

- Additional security and management is added.
- Logical links conserve physical ports.
- Depending on the protocol, multimode configurations can be implemented.
- Routers control access to VLANs.
- Up to 255 VLANs or more can be supported per router.

Router interface and Subinterface Comparison

- **Port Limits**
- **Performance**
- **Access ports and Trunk ports**
- **Cost**
- **Complexity**

Physical Interface	Subinterface
One physical interface per VLAN	One physical interface for many VLANs
No bandwidth contention	Bandwidth contention
Connected to access mode switch port	Connected to trunk mode switch port
More expensive	Less expensive
Less complex connection configuration	More complex connection configuration

Switch Security

Important to secure the switches and have a basic knowledge of:

- **Passwords**
- **Common security attacks**
- **Port security and unused ports**

Passwords

- **Secure the console port of unauthorized access**

Cisco IOS CLI Command Syntax	
Switch from privileged EXEC mode to global configuration mode.	`S1#configure terminal`
Switch from global configuration mode to line configuration mode for console 0.	`S1(config)#line con 0`
Set **cisco** as the password for the console 0 line on the switch.	`S1(config-line)#password cisco`
Set the console line to require the password to be entered before access is granted.	`S1(config-line)#login`
Exit from line configuration mode and return to privileged EXEC mode.	`S1(config-line)#end`

Passwords

- **Secure the vty ports from unauthorized access**
- **Make sure to secure all available vty lines**

Cisco IOS CLI Command Syntax	
Switch from privileged EXEC mode to global configuration mode.	`S1#configure terminal`
Switch from global configuration mode to line configuration mode for vty lines 0 - 4.	`S1(config)#line vty 0 4`
Set cisco as the password for the vty lines on the switch.	`S1(config-line)#password cisco`
Set the vty lines to require the password to be entered before access is granted.	`S1(config-line)#login`
Exit from line configuration mode and return to privileged EXEC mode.	`S1(config-line)#end`

Passwords

- **Configure privileged EXEC mode passwords**
- **Clear text or encrypted**

Cisco IOS CLI Command Syntax	
Switch from privileged EXEC mode to global configuration mode.	`S1#configure terminal`
Configures the **enable password** to enter privileged EXEC mode.	`S1(config)#enable password` *password*
Configures the **enable secret** password to enter privileged EXEC mode.	`S1(config)#enable secret` *password*
Exit from line configuration mode and return to privileged EXEC mode.	`S1(config)#end`

Passwords

- **Configure all passwords as encrypted passwords**

```
…
line con 0
 password cisco
 login
line vty 0 4
 password cisco
 no login
line vty 5 15
 password cisco
 no login
!
end
S1#config terminal
S1(config)#service password-encryption
S1(config)#end
S1#Show running-config
…
control-plane
```

Common security attacks

- **MAC flooding attack**
  - **MAC table incorrect, overflow**
- **DHCP spoofing**
  - **Illegal DHCP server answer on DHCP requests**
- **CDP attacks**
  - **CDP information is sent as broadcasts**
  - **Information can be used to attack your network**

Port Security

- **Port security limits the number of valid MAC addresses on a switch port**
- **Implement port security on all switch ports to:**
  - **Specify a group of valid MAC addresses allowed on a port**
  - **Allow only one MAC address to access the port**
  - **Specify that the port automatically shuts down if unauthorized MAC addresses are detected**

Unused ports

- **Disable all unused switch ports**

```
…
interface FastEthernet0/4
 shutdown
!
interface FastEthernet0/5
 shutdown
!
interface FastEthernet0/6
 shutdown
…
!
interface FastEthernet0/18
 switchport mode access
 switchport port-security
…
```