REDECOMEP

Redes Comunitárias de Ensino e Pesquisa

Soluções para Redes Metropolitanas

Emanoel Nigri
enigri@cisco.com

Cisco Catalyst 2950 Series
Standalone Devices for Lower Density Requirements

- Wire speed performance layer 2 switching with intelligent services
- Choice of software images:

  Enhanced Image – Intelligent Services

  Standard Image – Baseline Cisco IOS Functionality
- Choice of Ethernet interface speed and media type
- Ease of deployment and management
- Proven IOS software

Cisco Catalyst 2970 Series
10/100/1000 Optimized

High-performance workgroups and small branch offices

- Standalone, layer 2 fixed-configuration switch with intelligent services
- 10/100/1000 optimization with wire-speed switching enables Gigabit Ethernet everywhere
- Catalyst 3550 and 3750 are recommended choices for routing and stacking capabilities

Cisco Catalyst 3560 Series
High-performance Fixed Configuration

Small Power over Ethernet enabled wiring closet switches

- Power over Ethernet with Intelligent Power Management
- Wire speed 10/100 and GbE configurations for switching and routing
- High-performance switching and routing
- Intelligent Layer 2, 3, 4 services

Cisco Catalyst 3750 Series
Revolutionizing Stackable Switching

Unified Stacking, Behaving as a Single Unit

- Industry's highest performance Stackable
- Revolutionary StackWise technology brings unparalleled stackable resiliency and capacity
- High-Performance 10/100/1000 optimization enables Gigabit Ethernet everywhere
- 10 Gigabit Uplinks for increased performance

Cisco Catalyst 4500 Series
High-performance Mid-range Chassis Solution

Resiliency & Control for Converged Networks

- Highest density 10/100/1000 mid-range Chassis
- Enables Redundancy everywhere in the network
- Only mid-range chassis delivering High-density, integrated in-line power
- Supervisor II-Plus extends reach to SMB and Education customers
- Proven investment protection through evolutionary design

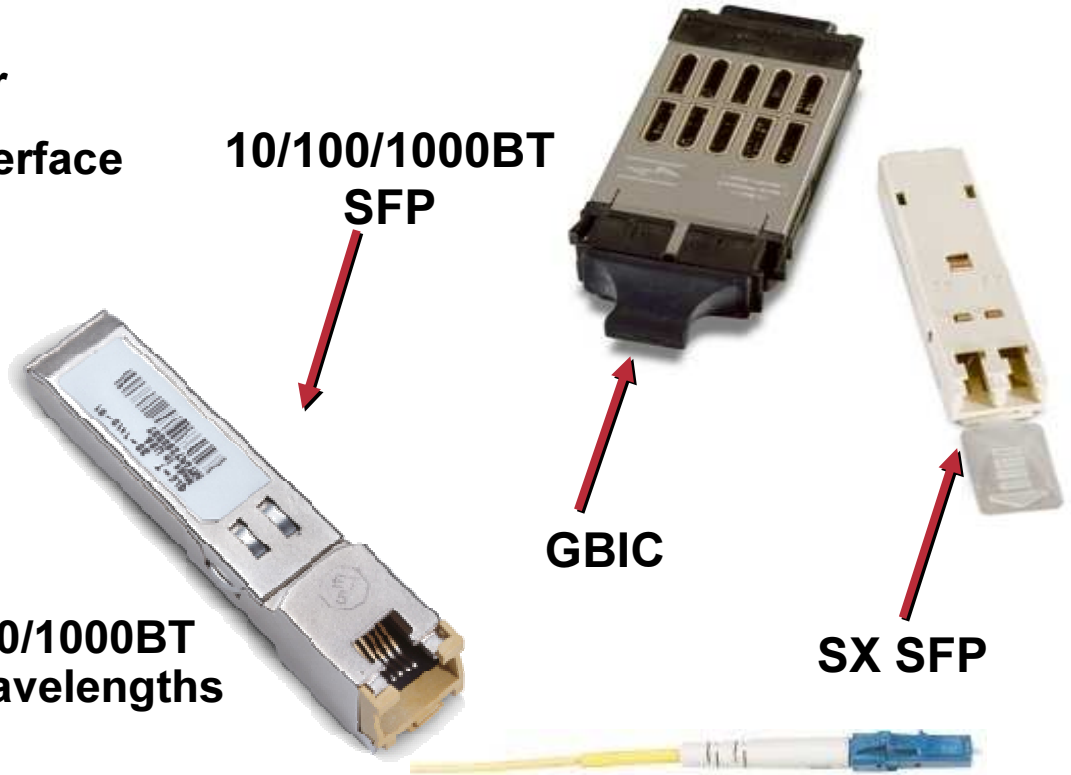
Cisco Catalyst 6500 Series
Industry's Most Flexible Modular Platform

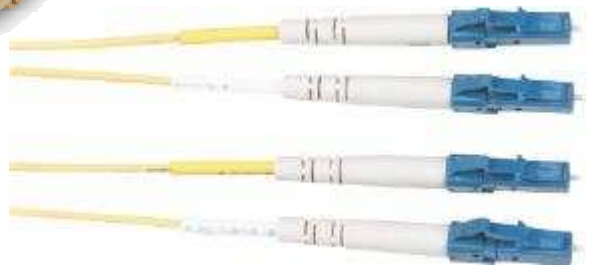
Evolutionary Innovation

- Evolutionary infrastructure
- Highest performance and non-stop application delivery
- Highest density 10GbE Aggregation
- Highest Density 10/100 and 10/100/1000 density in industry
- Integrated Advanced Services for greater extensibility

Small Form Factor Pluggable (SFP)

- New industry standard connector
- Same functionality as Gigabit Interface Converters (GBICs)
- Same specs as GBICs
- Hot pluggable
- Smaller fiber connector: LC for SF
- 2.5 SFPs fit in space of one GBIC
- Shipping Cisco SX, LX, ZX, 10/100/1000BT and CWDM versions in 8 color wavelengths





LC connectors

Fiber Gigabit Interface Converter (GBIC)

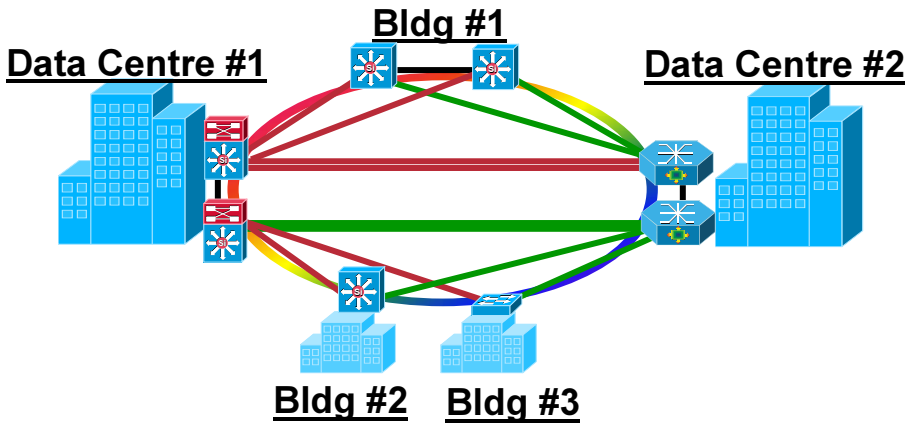
GBIC Port Cabling Specifications

GBIC	Wavelength (nm)	Fiber Type	Core Size (micron)	Modal Bandwidth (MHz/km)	Cable Distance
SX	850	MMF	62.5	160	722 feet (220 meters)
(WS-G5484)			62.5	200	902 feet (275 meters)
			50.0	400	1640 feet (500 meters)
			50.0	500	1804 feet (550 meters)
LX/LH	1310	MMF	62.5	500	1804 feet (550 meters)
(WS-G5486)			50.0	400	1804 feet (550 meters)
			50.0	500	1804 feet (550 meters)
		SMF	8.3/9/10	–	6.2 miles (10 km)
ZX	1550	SMF	8.3/9/10	–	43.5 miles (70 km)
(WS-G5487)			8	–	62.1 miles (100 km)

1000BASE-T GBIC (WS-G5483=)

- **Hot Swappable**
- **Support Auto MDIX**

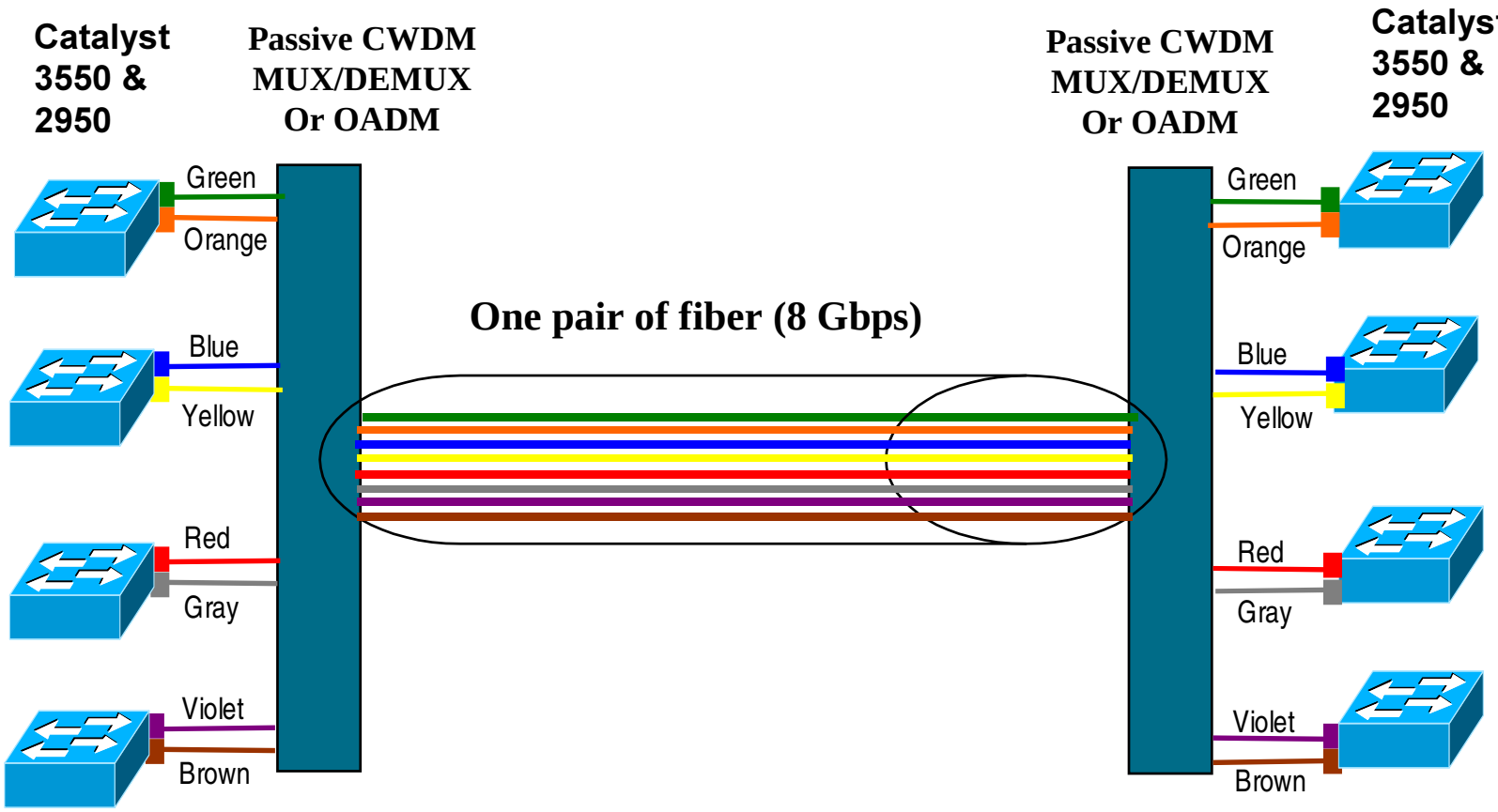
CWDM Networking



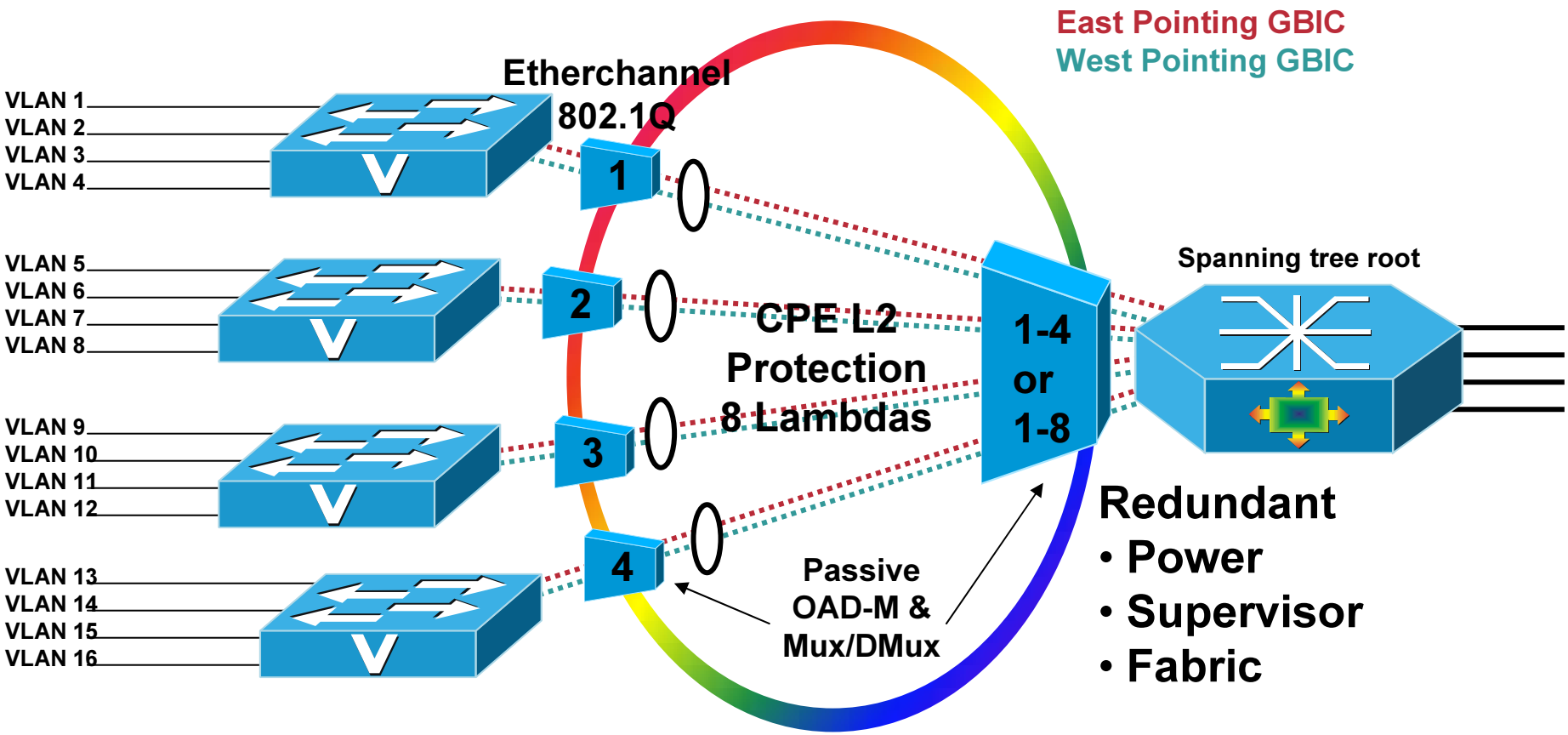
CWDM GBICs

- Supports point to point and ring topologies
- "ZX" distance (100 km)
- Allows up to 8 GbE interfaces mux'd with passive device
- Supports Multimodule EtherChannel for additional resiliency

CWDM GBIC Solution in Point-to-point Configuration



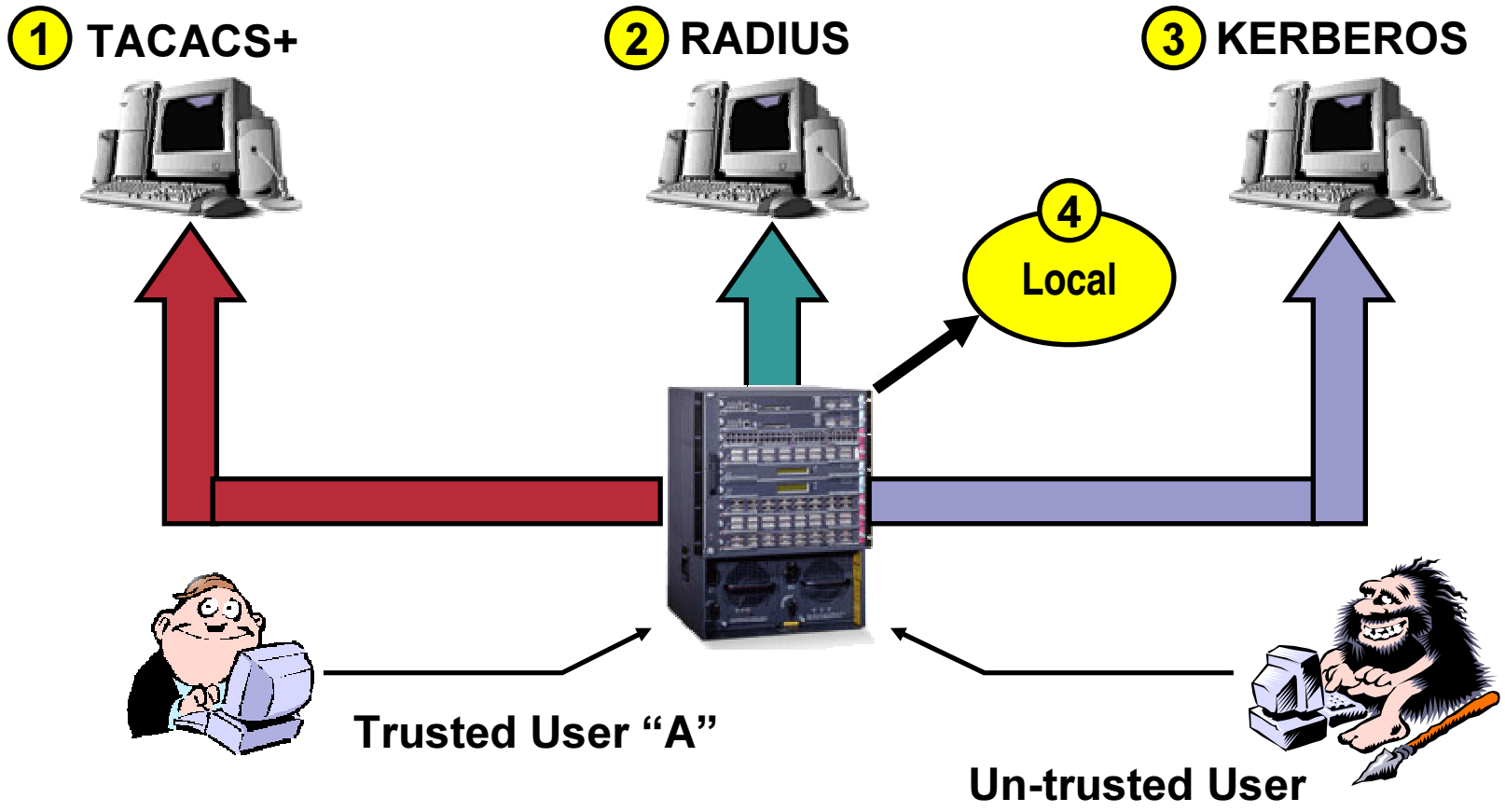
Gigabit Ethernet Metro Network High Availability Access – CWDM GBICs



Switch Features

Switch Access using AAA

There are four methods for providing authentication services on a switch and each method involves accessing an authentication server to validate the incoming access request from a user…



Privilege Levels

Privilege Levels

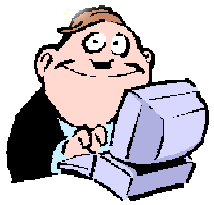
15 High
14
13
12
11
10
9
8
7
6
5
4
3
2
1
0 Low

Assign privilege levels to commands, THEN…
Assign privilege levels to enable passwords, VTY (Telnet) lines and the console
Defines which commands can be executed by which ports

Can define user "A" with higher privilege level providing access to more commands

Can define user "B" with lower privilege level providing access to fewer commands

Secure Shell (SSH)



Generate RSA public and private key

Initiate Telnet Request

Server sends its RSA public key

Client encrypts a random session key and sends back to server

Server decrypts message using its own private key

Subsequent session is encrypted

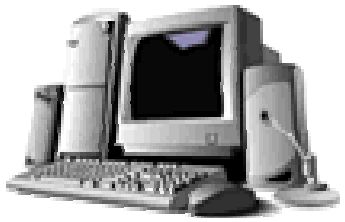
The session key is used by whichever cipher is chosen for encryption. Since only the client and a server running on a machine that knows the secret half of the server's host key can know the session key, this both secures the session, and assures the client that it must be talking to the correct server machine.

SNMP V3 Security

Cisco.com

SNMP can obtain information from your switch that are contained in the various MIB's

SNMP Server



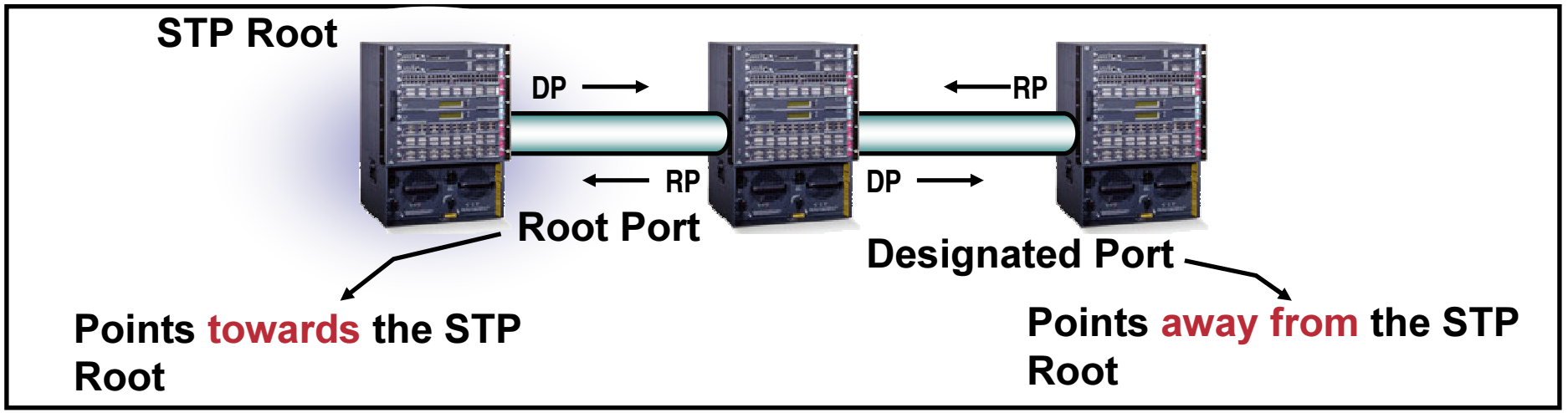
SNMP Data

Potential security exposure on the network

Switch

Model	Level	Authentication	Encryption	What Happens
V1	noAuthNoPriv	Community String	No	Community string match to authenticate
V2c	noAuthNoPriv	Community String	No	Community string match to authenticate
V3	noAuthNoPriv	Username	No	Username match to authenticate
V3	AuthNoPriv	MD5 or SHA	No	MD5 or SHA-1 authentication
V3	AuthPriv	MD5 or SHA	DES	MD5 or SHA-1 authentication and DES to encrypt SNMP data

Spanning Tree Rootguard



Enhances the security of your STP configuration in your network…

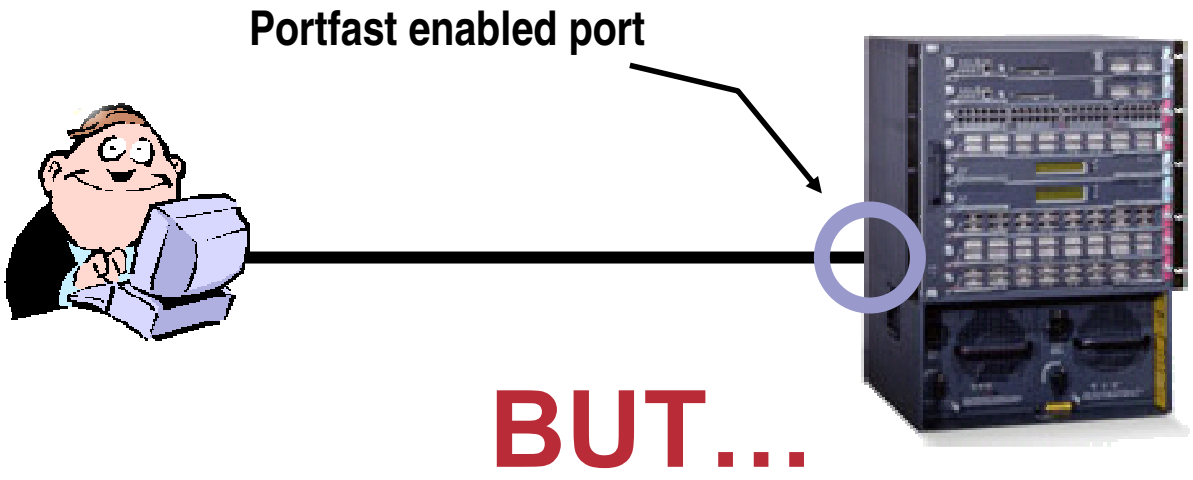
Denies a non authorized switch from assuming the STP Root role which if allowed on the wrong device can impact performance…

HOW DOES IT WORK???

Rootguard forces a port to be a DESIGNATED port so that no other switch can become the STP Root…

Portfast BPDU Guard

Portfast is a Spanning Tree enhancement that is set on a switch port that typically connects to a host… {Portfast bypasses STP states of listening and learning to decrease the time it takes to activate a port)

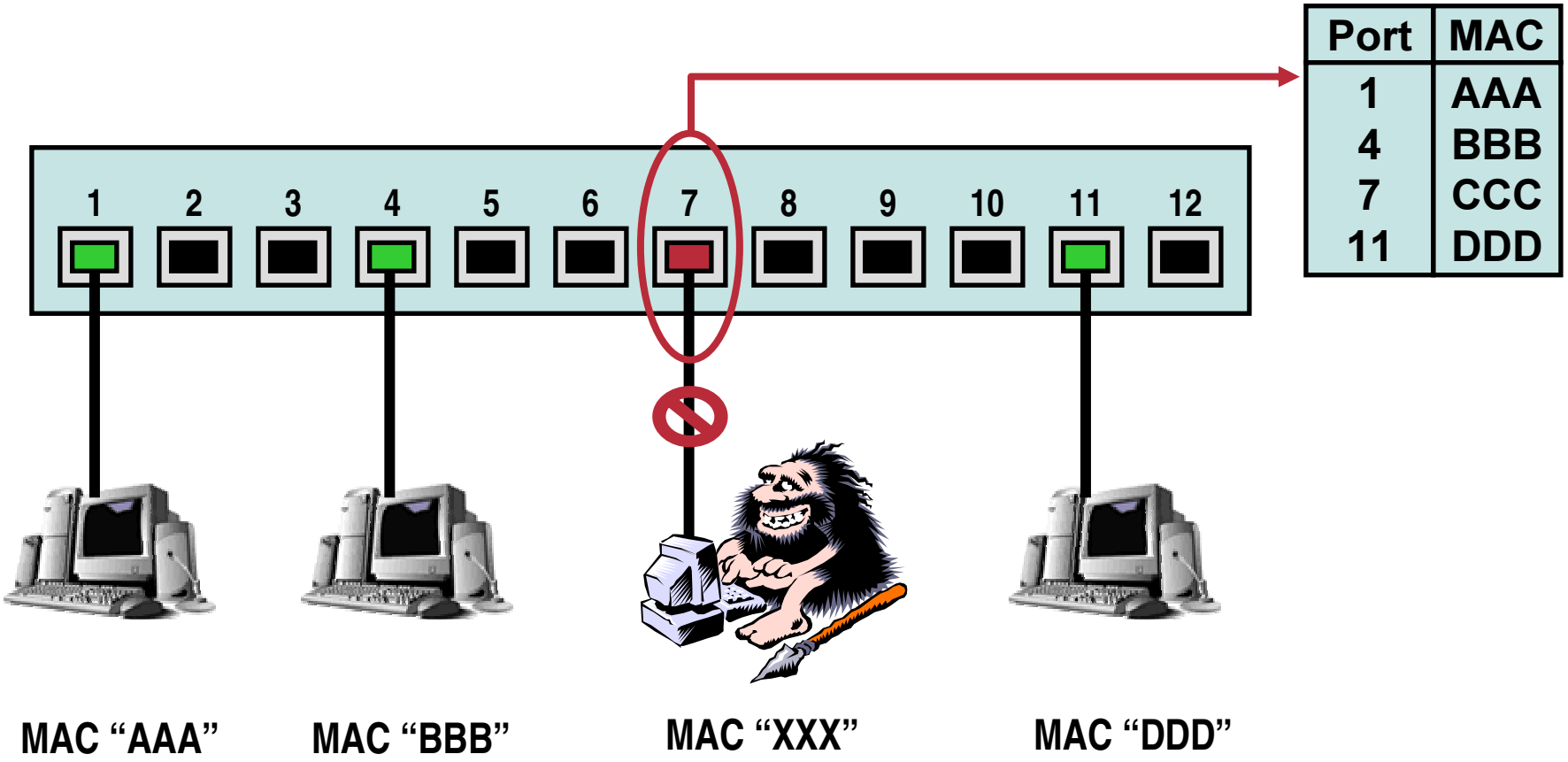


…if a switch were now connected to the same port in place of the user, a spanning tree loop could result in the switch network falling over…

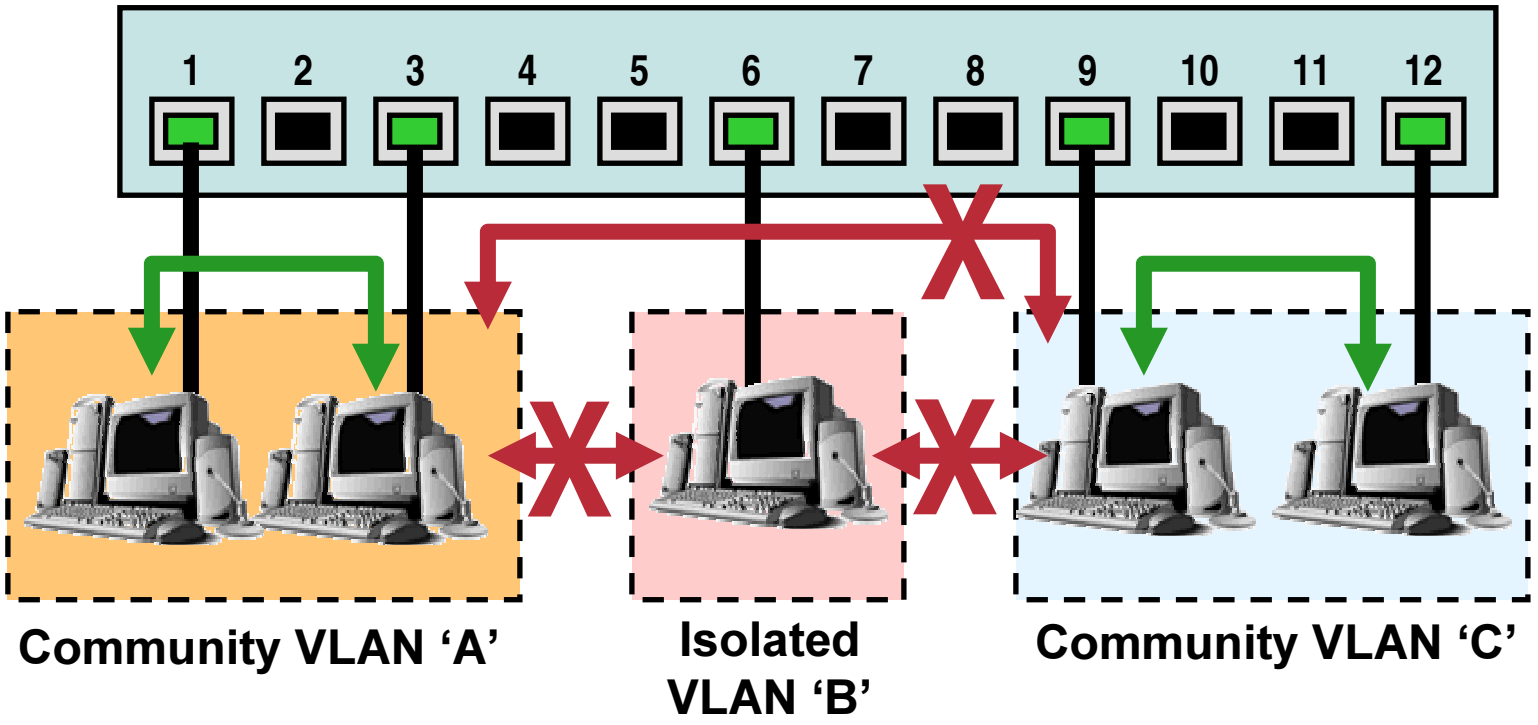
This equates to a DENIAL OF SERVICE for all attached hosts in that Spanning Tree domain…

Port Security

Defines a way to secure a port by MAC address so that only the device with that MAC address can bring the link up…



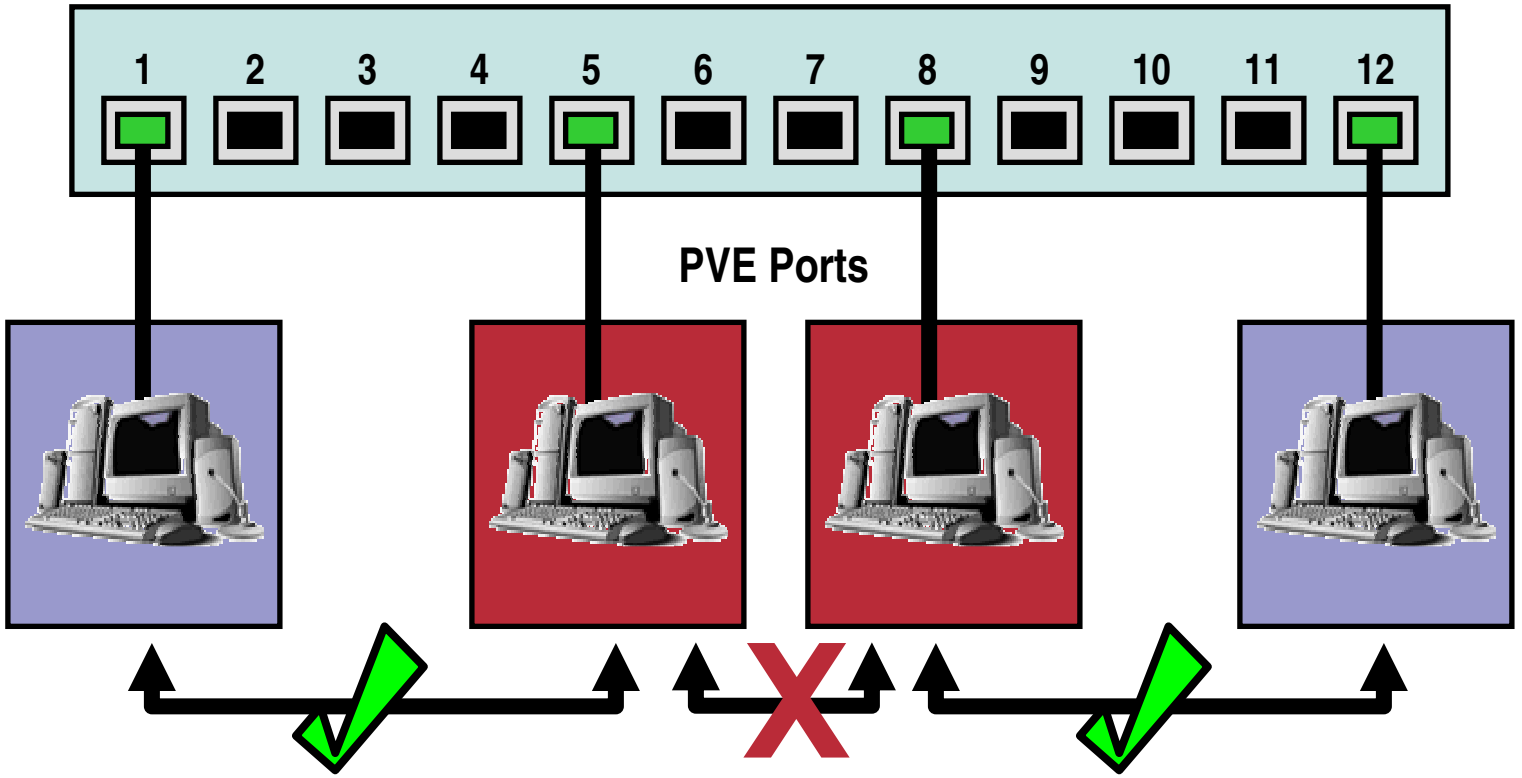
Private VLAN's



…Private VLAN's allows the creation of "sub-VLAN's" within a primary VLAN. These "sub-VLAN's" known as community VLAN's and Isolated VLAN's restrict the movement of traffic while allowing the use of the same subnet address space. Communication outside of the "sub-VLAN" Can only take place via the promiscuous port…

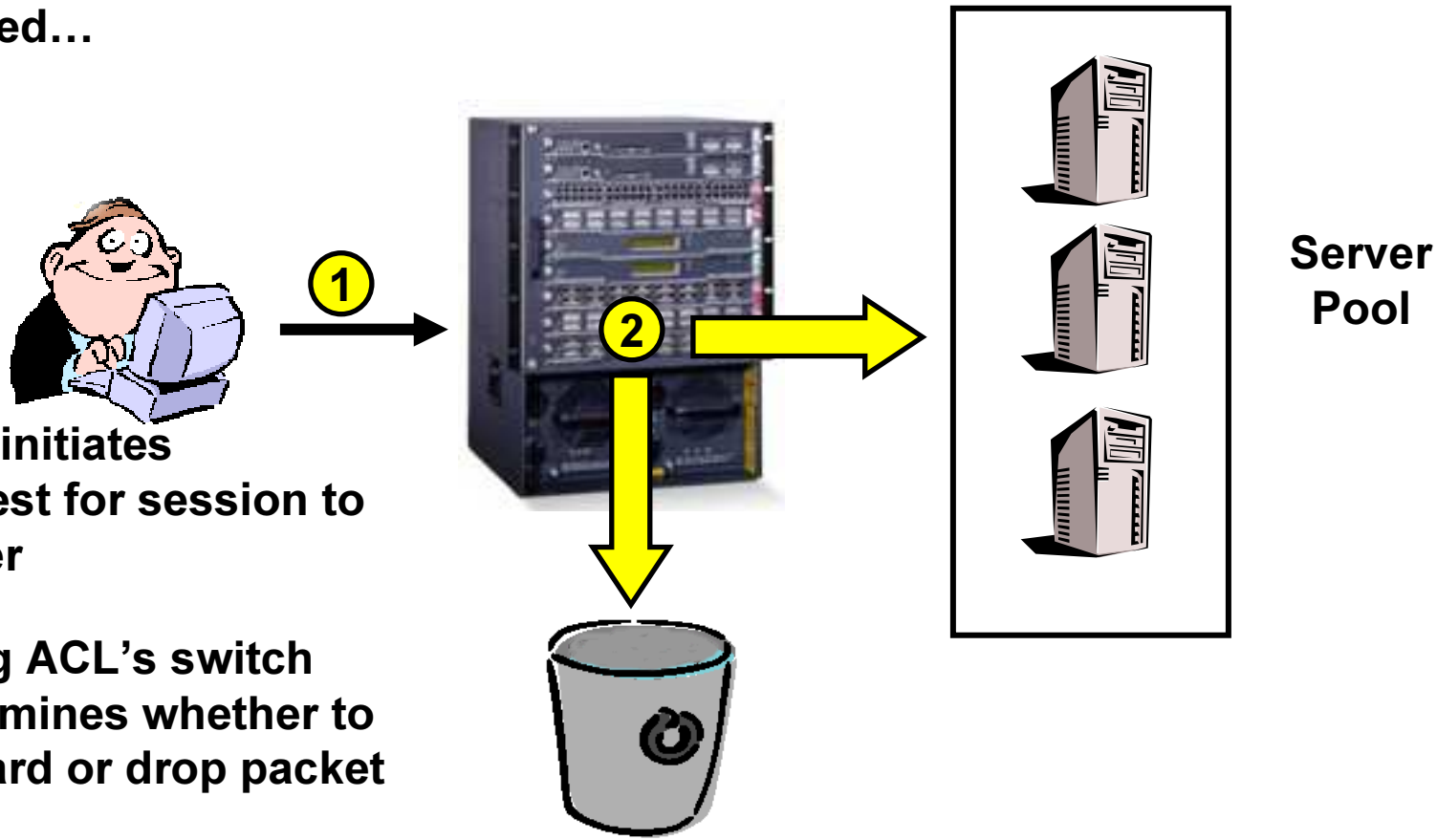
Private VLAN Edge

...Private VLAN Edge (PVE) allows the creation of "isolated" ports. Forwarding of unicast, multicast and broadcast traffic between isolated ports is prohibited. Forwarding of traffic from isolated ports to normal ports is performed as per normal...



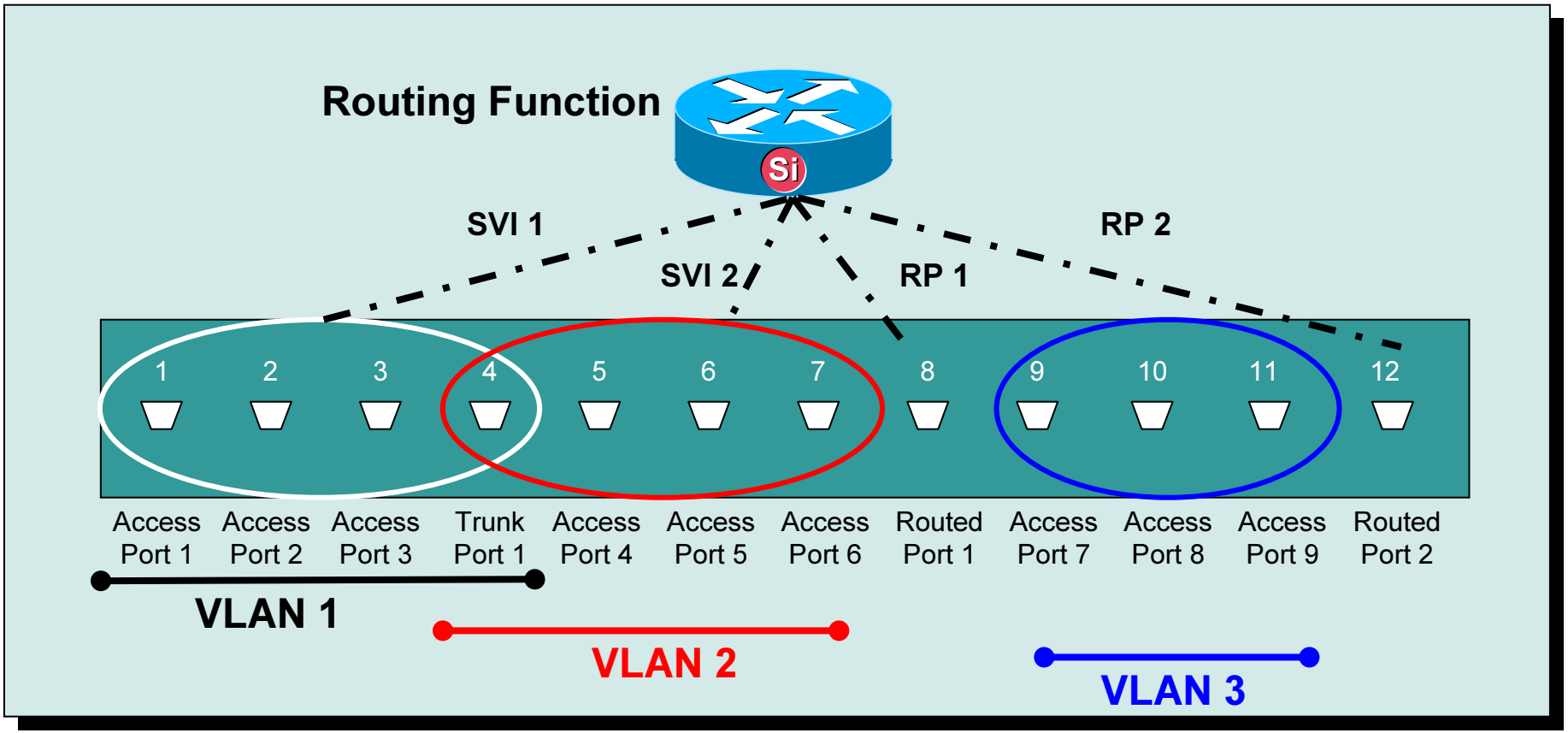
Access Control Lists

Access Control Lists (ACL's) provide a mechanism to inspect the contents of a packets header to assist in determining whether a packet is forwarded or dropped…

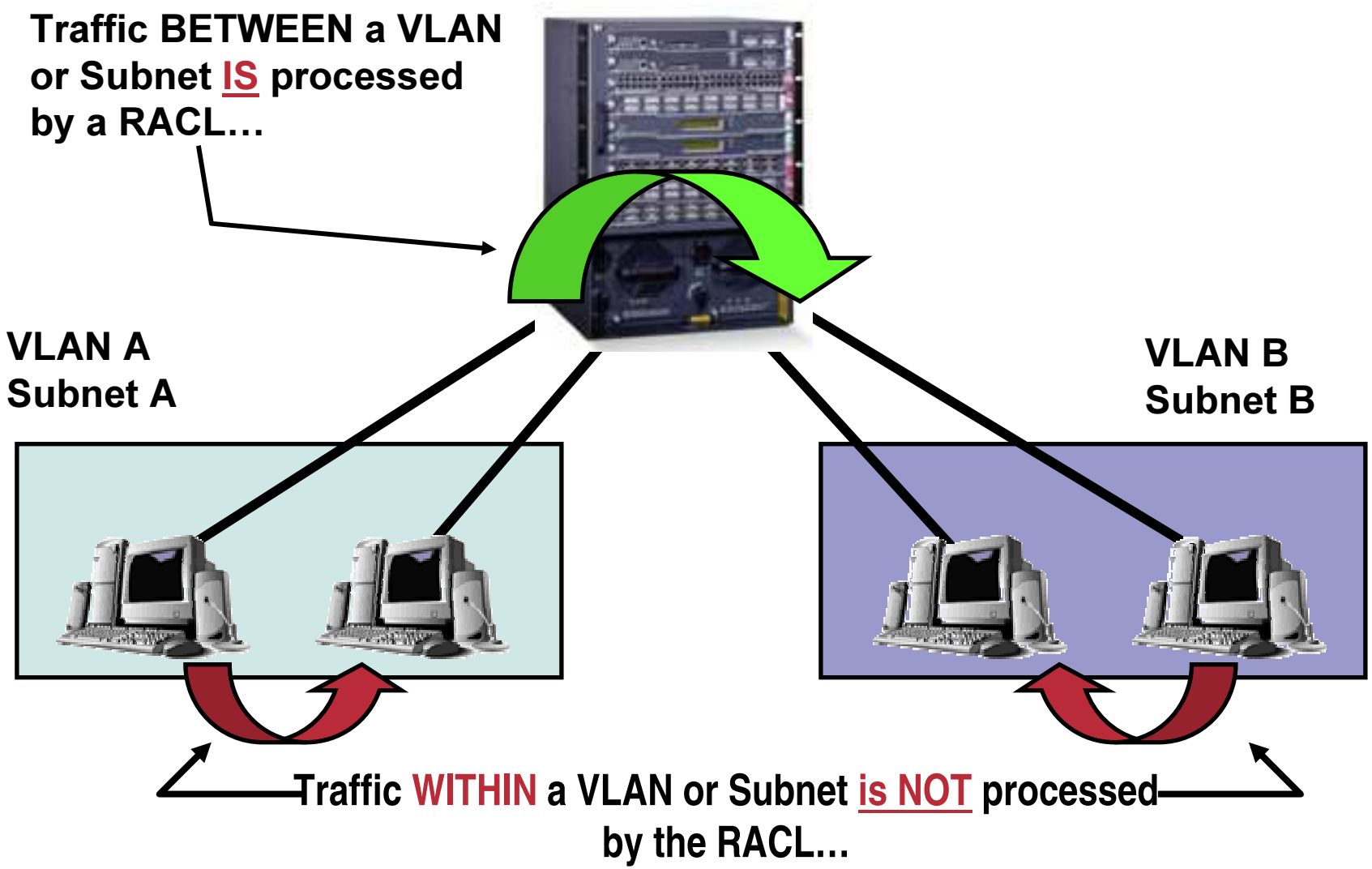


1. **User initiates request for session to server**
2. **Using ACL's switch determines whether to forward or drop packet**

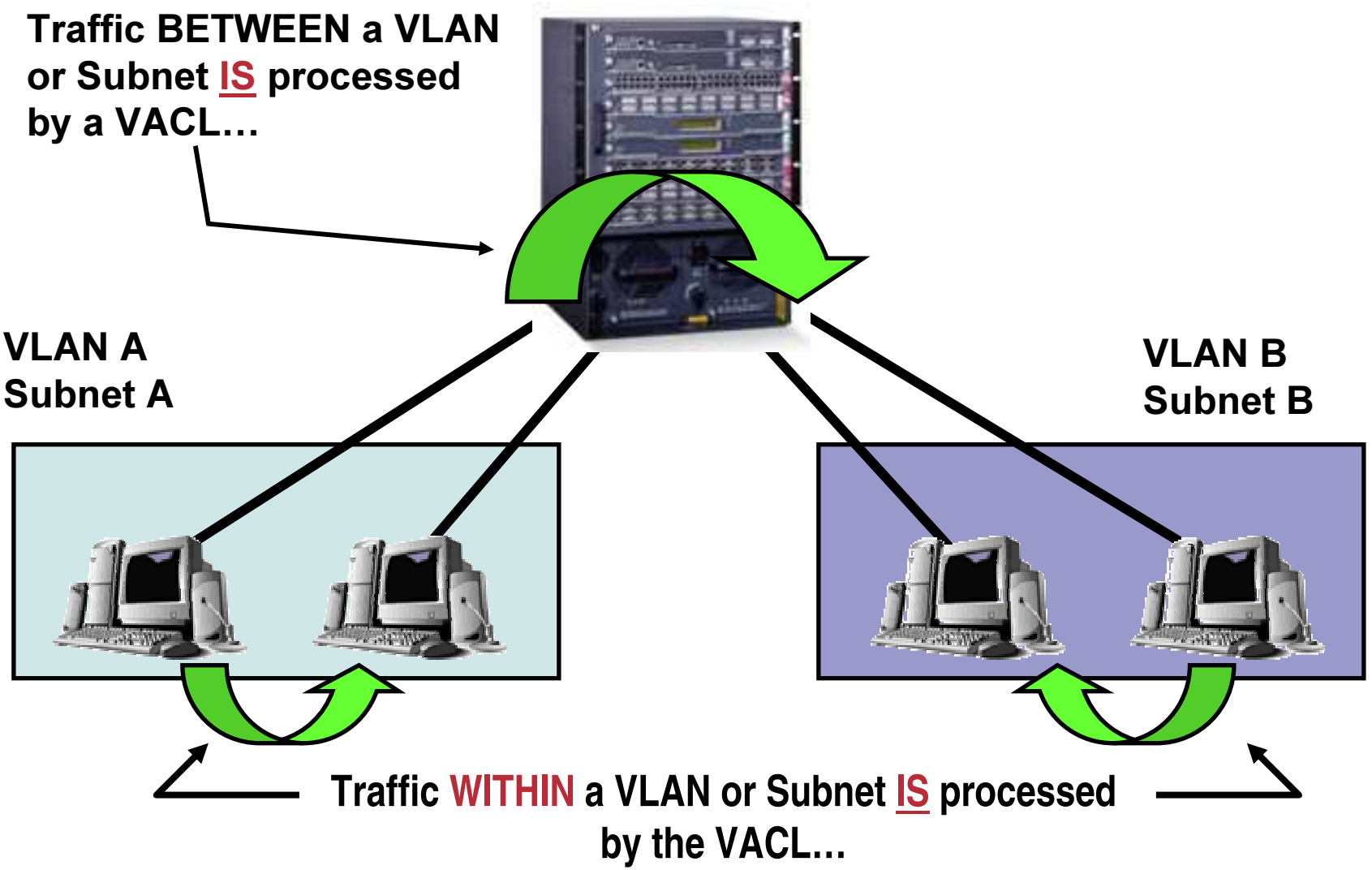
Interface Summary in Cisco IOS



Router Access Control Lists



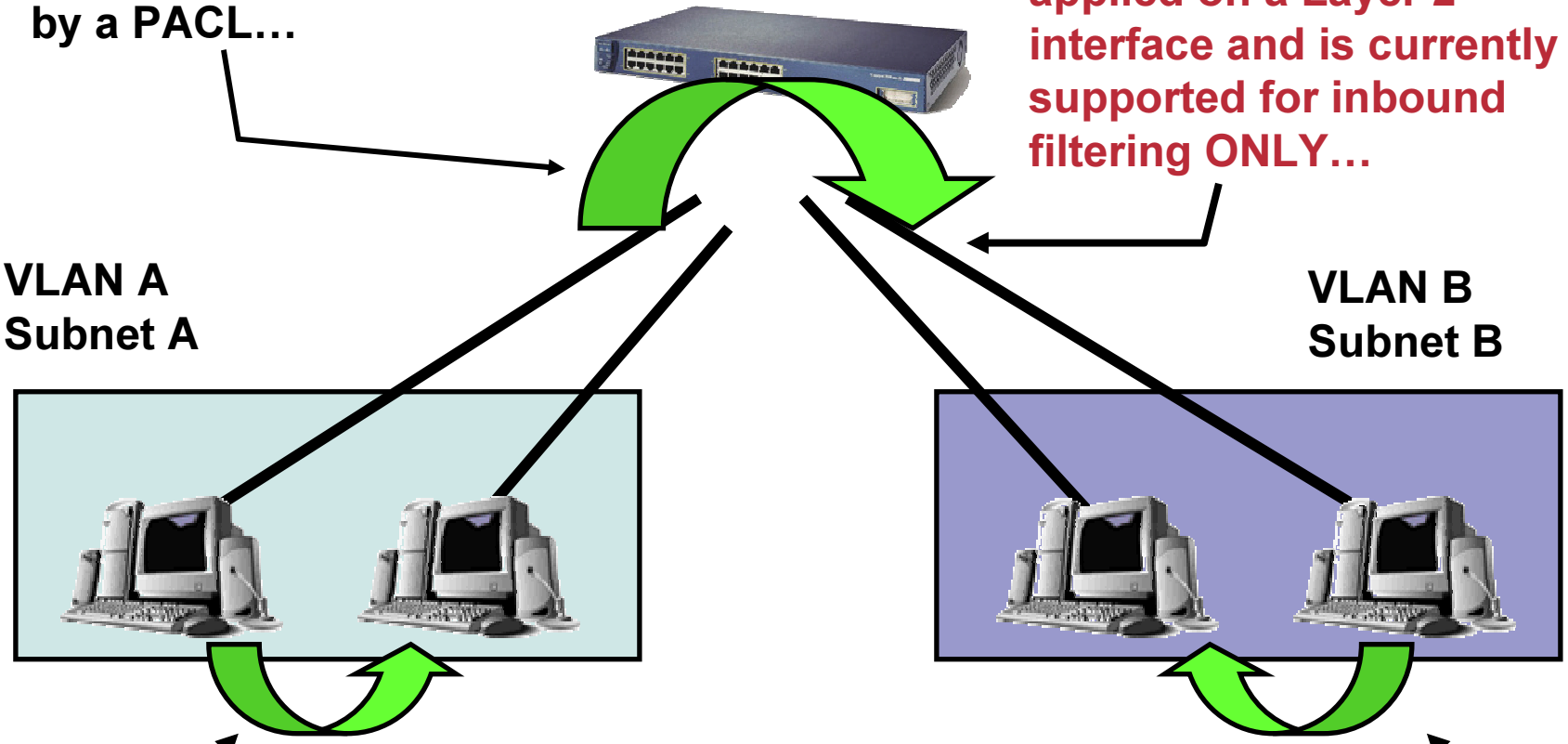
VLAN Access Control Lists



Port Access Control Lists

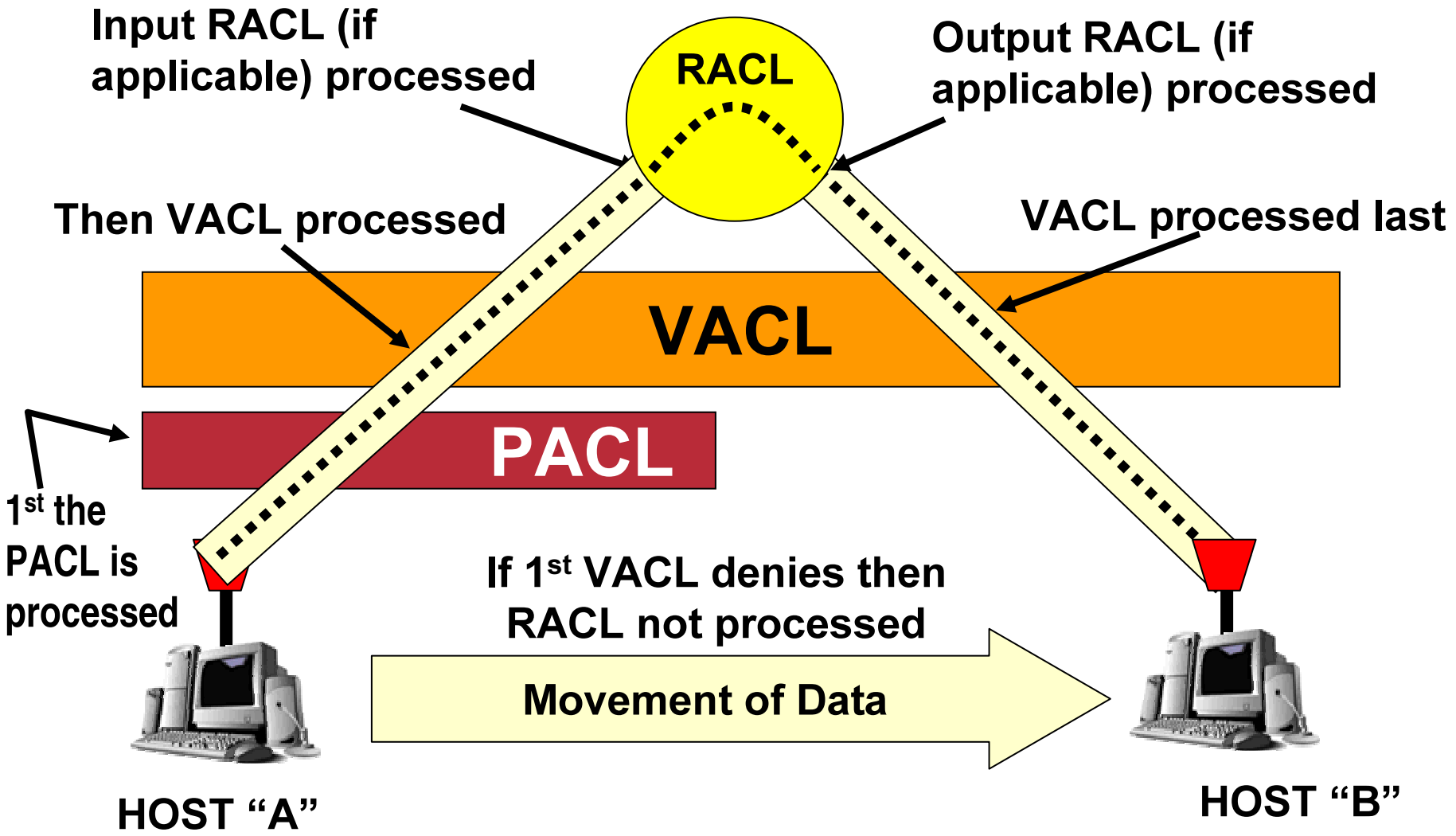
Traffic BETWEEN a VLAN or Subnet IS processed by a PACL…

KEY POINT – PACL is applied on a Layer 2 interface and is currently supported for inbound filtering ONLY…



Traffic WITHIN a VLAN or Subnet IS processed by the PACL…

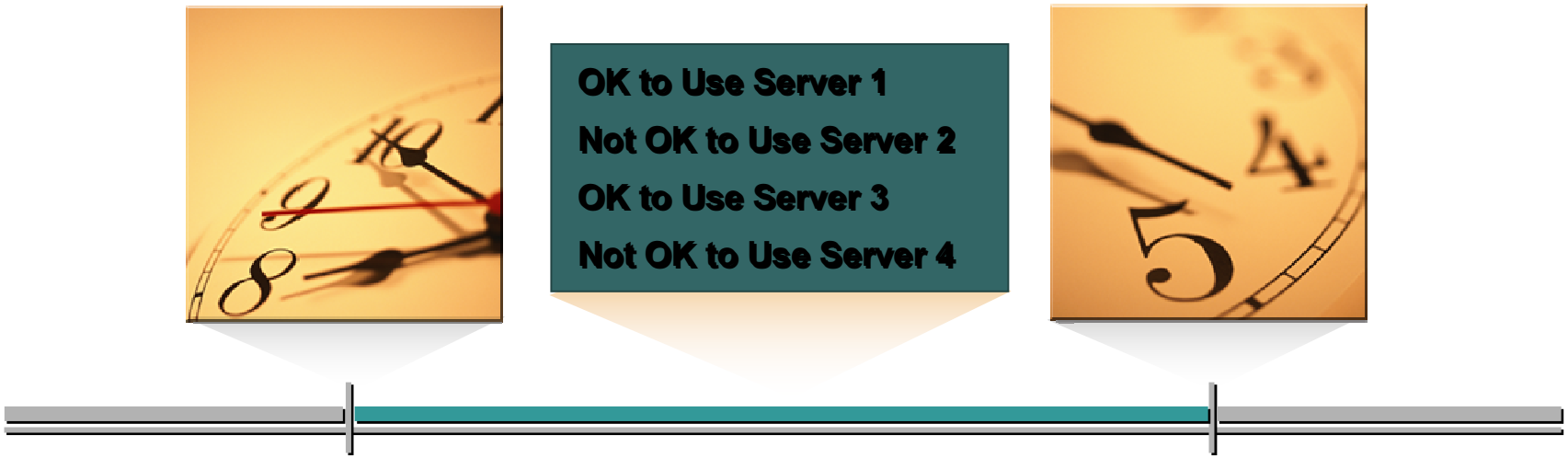
Using PACL, VACL and RACL's Together



Time-Based ACLs

How It Works:

Controls the switching of data based on the time of day.



ACL goes on at 8:00 AM

ACL goes off at 5:00 PM

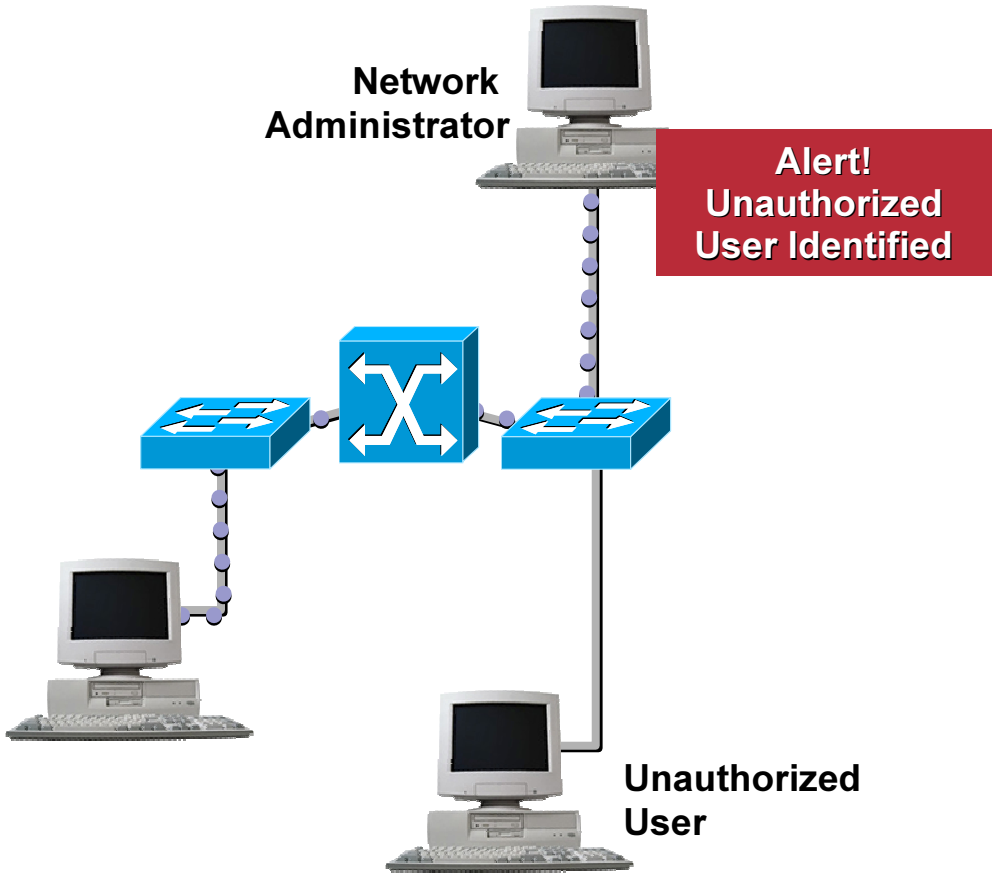
Notification for Intrusion

- **ACL Logging**

  Tracks ACL violations that occur in a network; the user's MAC address can be obtained to assist in tracking the user's location.

- **MAC Address Notification**

  Alerts network administrators if unauthorized users come on to the network.



Rate Limiting (Policing) QoS ACLs

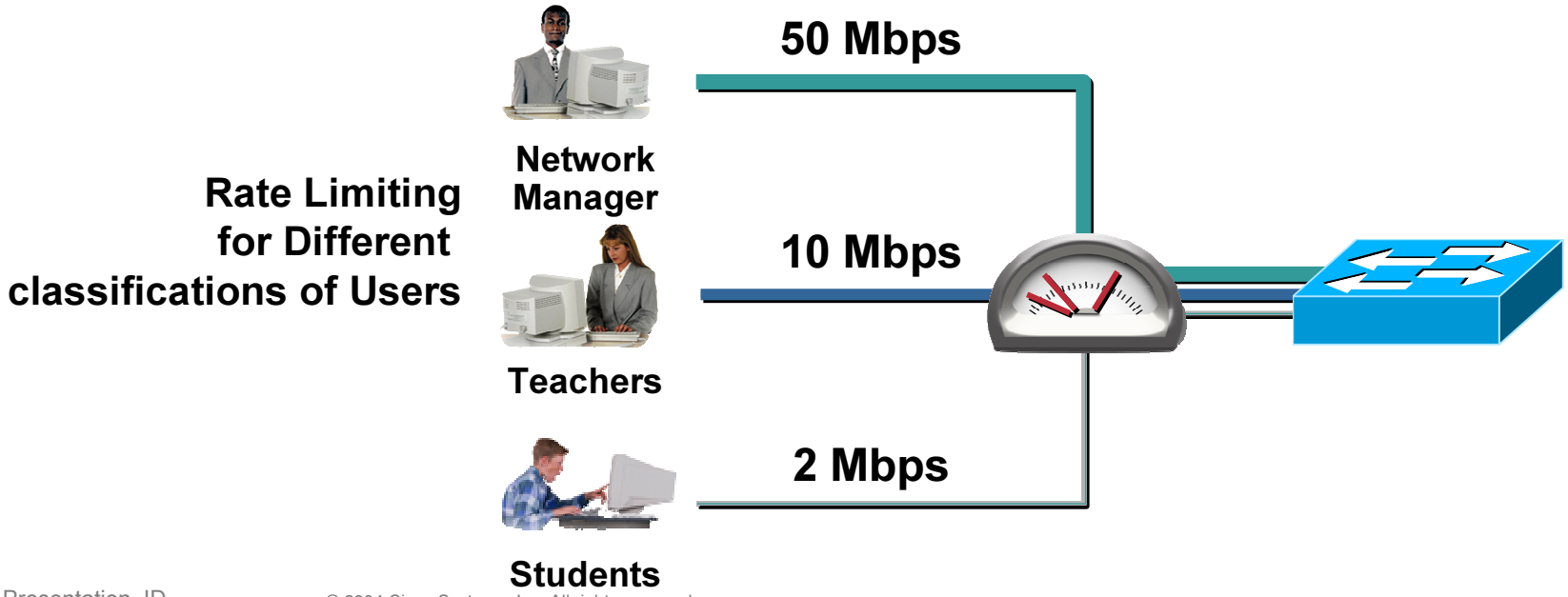
What It Does:

Allows network managers to set bandwidth thresholds for users and by traffic type.

Benefits:

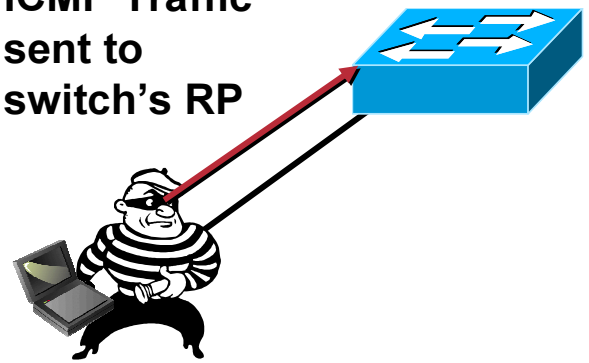
Prevents the deliberate or accidental flooding of the network.

Keeps traffic flowing smoothly.



Control Plane Policing (CPP) on the Catalyst 6500

100 Mbps of ICMP Traffic sent to switch's RP



Problem:

- DoS Attacks at infrastructure devices generate rogue IP traffic streams destined to the Route Processor at very high data rates.
- Affects routing protocols, STP updates, which in turn severely affect network stability

Traffic bound for processor rate limited

Solution:

Route Processor Rate Limiting provides hardware-based mechanism for limiting traffic destined to RP, including:

Ingress/Egress ACLs

CEF Receive and Glean

ICMP Redirects/Unreachable

TTL Failure

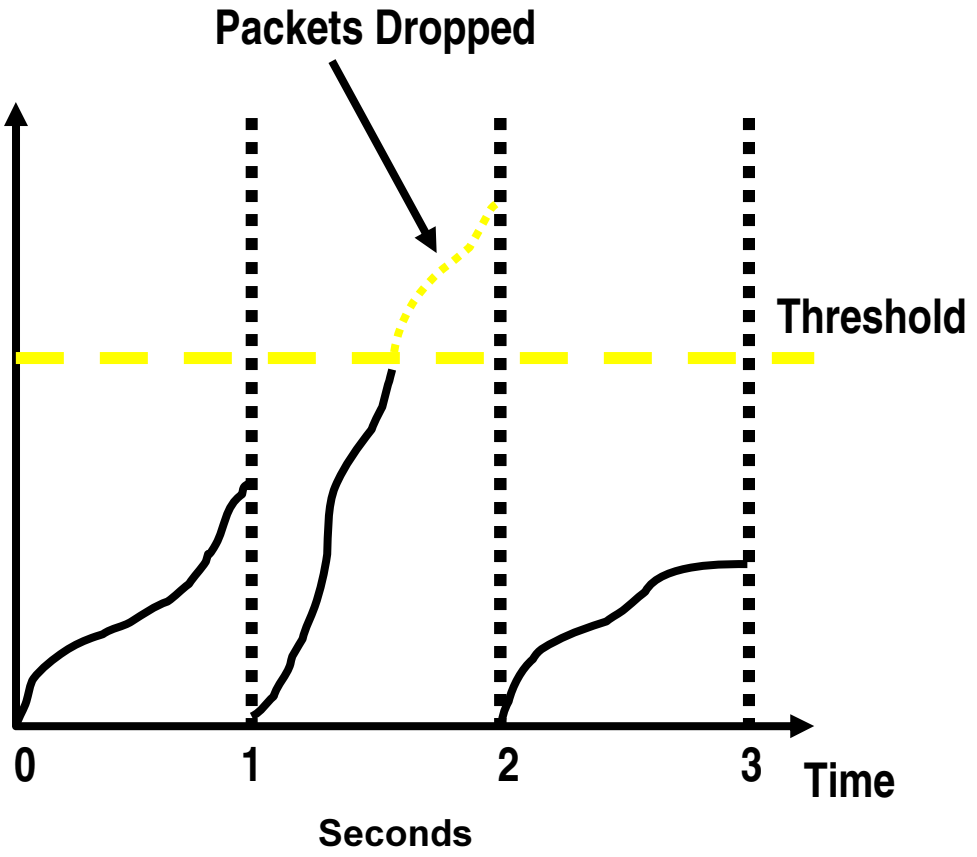
CEF No Route

RPF Failure

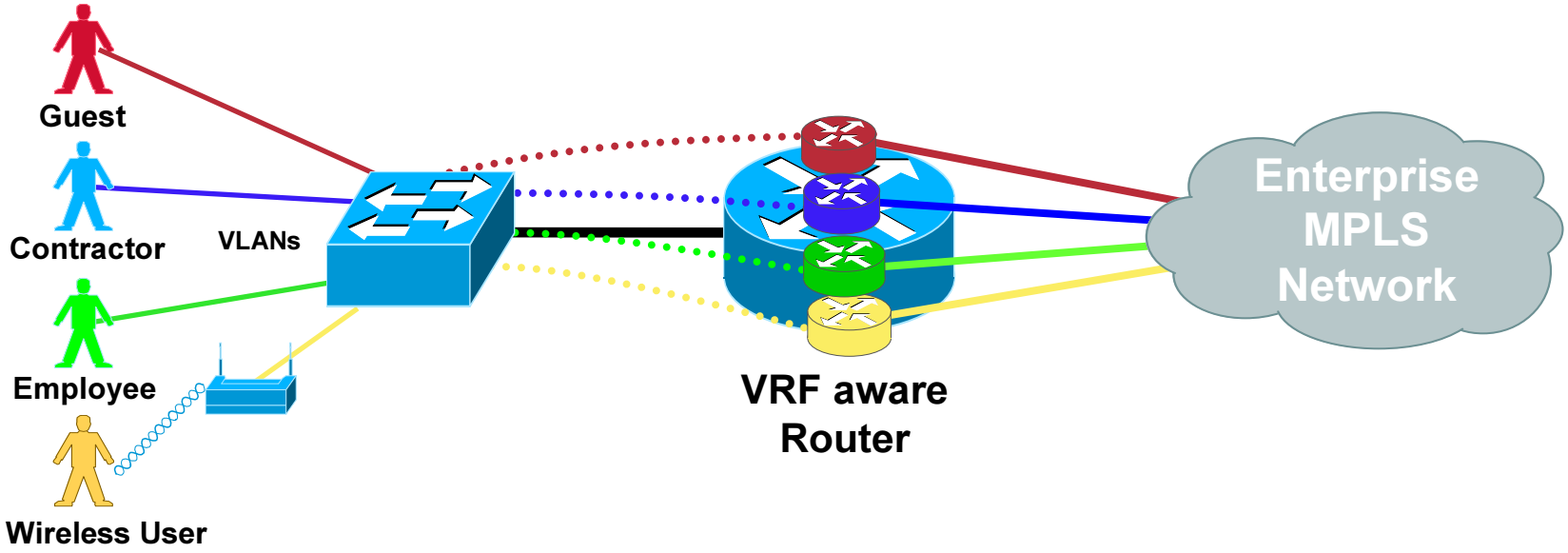
VACL Logging

Broadcast Suppression for Storm Control

- Storm Control is also known as Broadcast suppression
- Able to limit the volume of broadcast, multicast and/or unicast traffic
- Protect the network from intentional and unintentional flood attacks i.e. STP loop
- Limit the combined rate of broadcast & multicast traffic to normal peak loads



Virtual Route Forwarding (VRF)-Lite



- **What it Does**

  VRF-Lite provides a private forwarding table per VPN on the LAN switch. This can in turn map to an MPLS VPN (RFC-2547)

- **Benefit**

  Privacy in the network can be enforced in the wiring closet


Cisco Systems