Network Access, Security and VLANs

Lecture 3

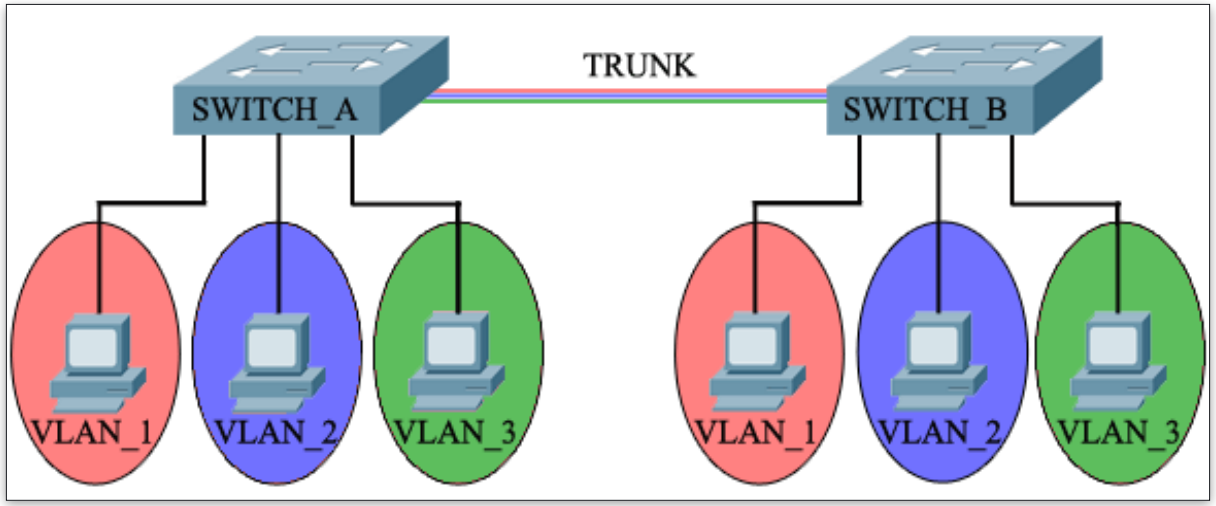
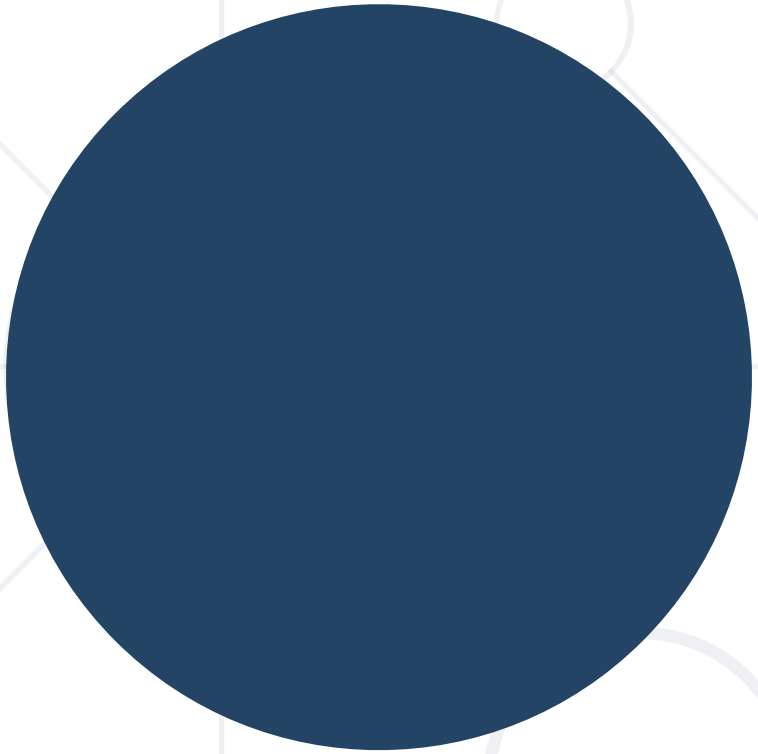


Table of Contents



Device memory components

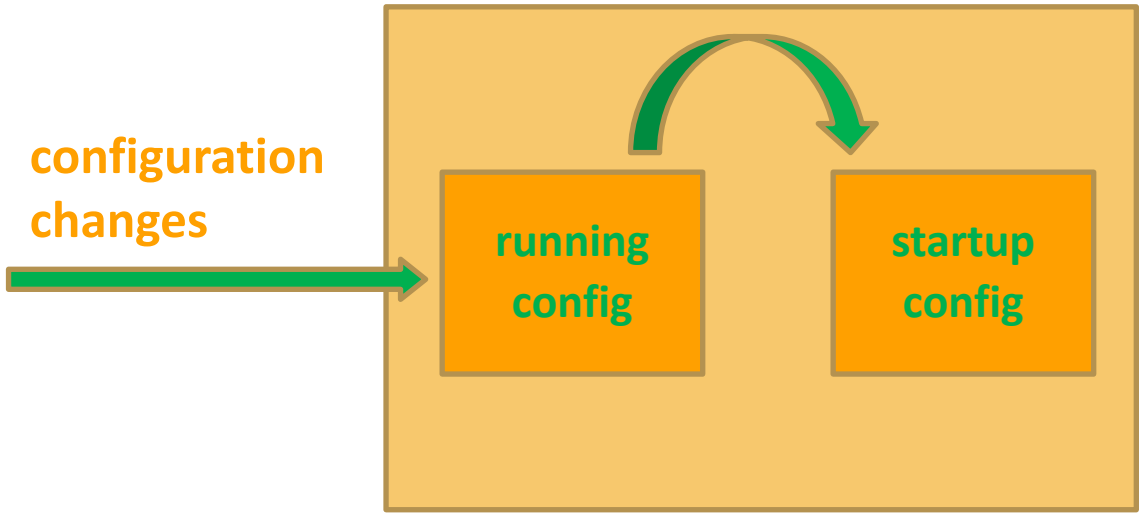
Main memory components in a network device

- RAM (Random Access Memory)
  - stores the running configuration file
  - loses content when the power goes down
- NVRAM (NonVolatile RAM)
  - stores the startup configuration file
  - retains content when the power goes down

Main memory components in a network device (2)

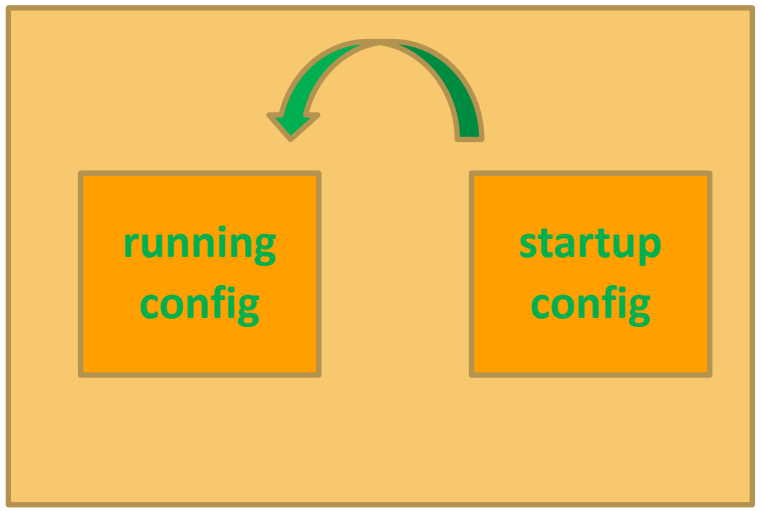
- Flash memory
  - stores the device image (operating system)
  - retains content when the power goes down
- ROM (Read-Only Memory)
  - maintains instructions for power-on self test (POST) diagnostics
  - Stores bootstrap program and basic operating system software
  - retains content when the power goes down

Saving the configuration

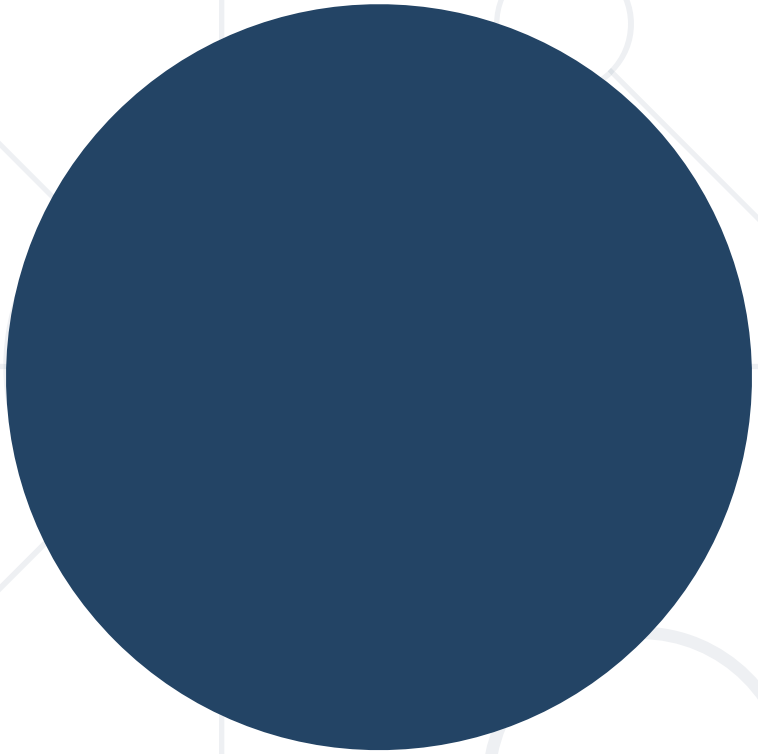


- The configuration file must be saved to survive reboot
- To save the running configuration file (stored in RAM) to the startup configuration file (stored in NVRAM), use either:
  - copy run start
  - write memory

Loading the configuration



- The saved configuration file (startup config file) will go in the RAM (the running config file) when:
  - the device is restarted
  - a copy start run command is executed

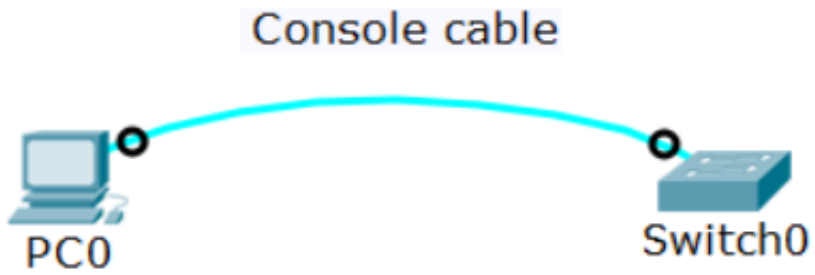


Accessing network devices

Out-of-band vs in-band management

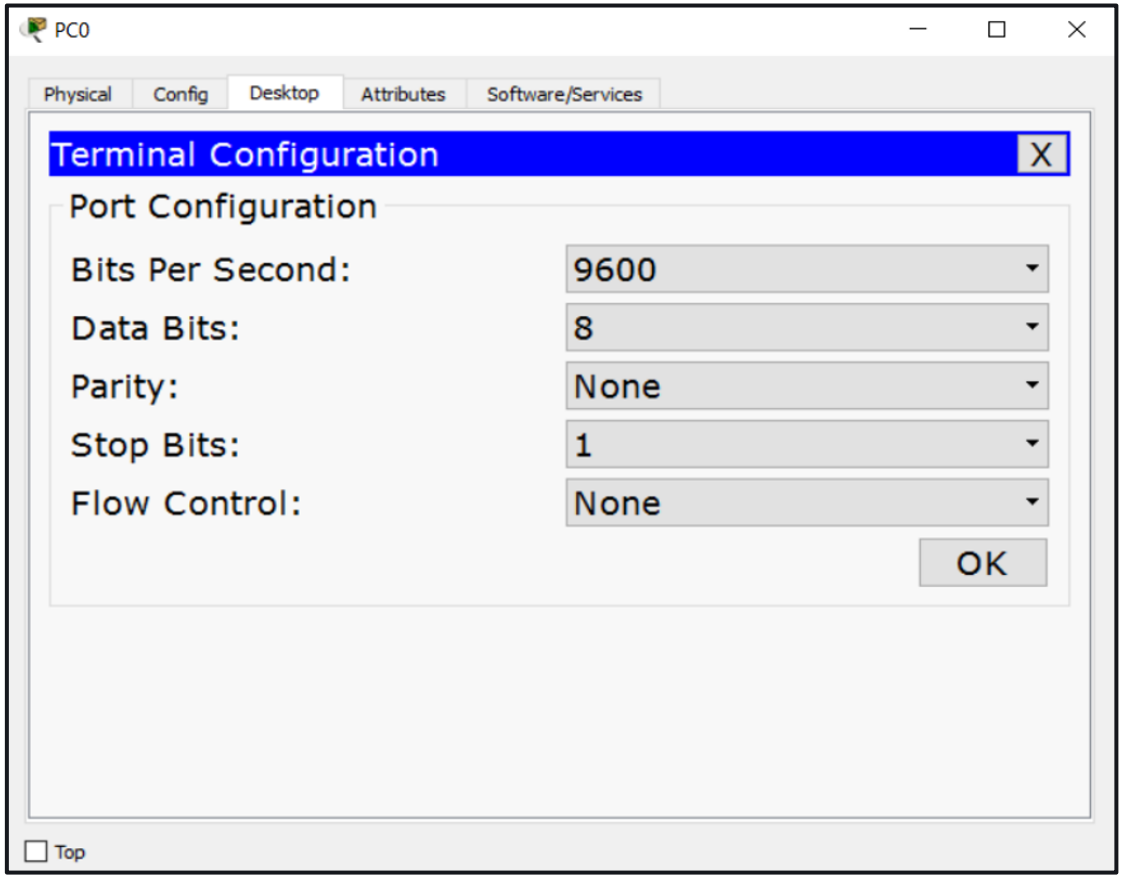
- Out-of-band:
  - Management traffic uses separate path from the user traffic
  - Typical protocol: Console
- In-band management
  - Management traffic travels the same path as user traffic
  - Typical protocols: Telnet, SSH, SNMP, Web

Out-of-band management



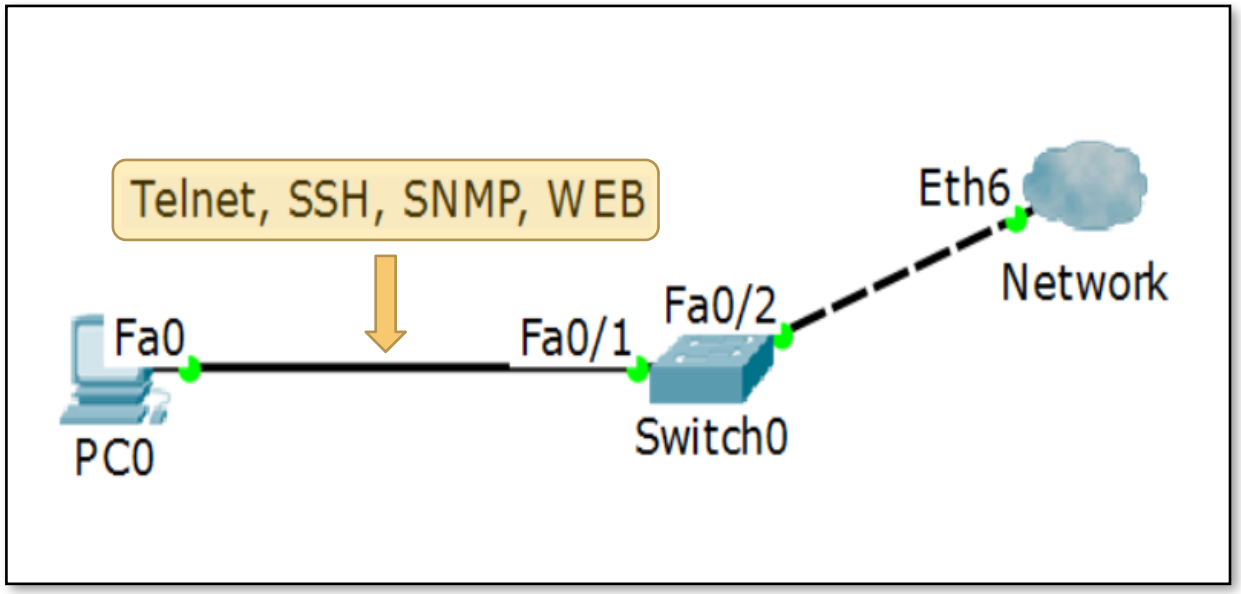
- Dedicated channel for management only
- Needs terminal emulator software (Putty, SecureCRT, etc.)
- No IP addresses are required
- More secure & reliable for management
- Traffic is local and not routed

Out-of-band management (2)



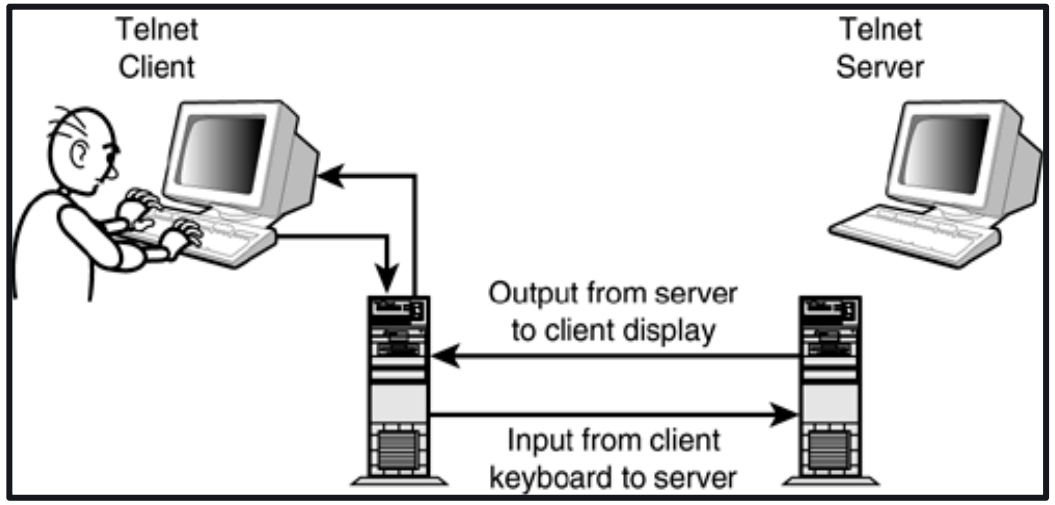
- Typical default configuration for a terminal emulator
- Consult the device documentation if not using the defaults

In-band management



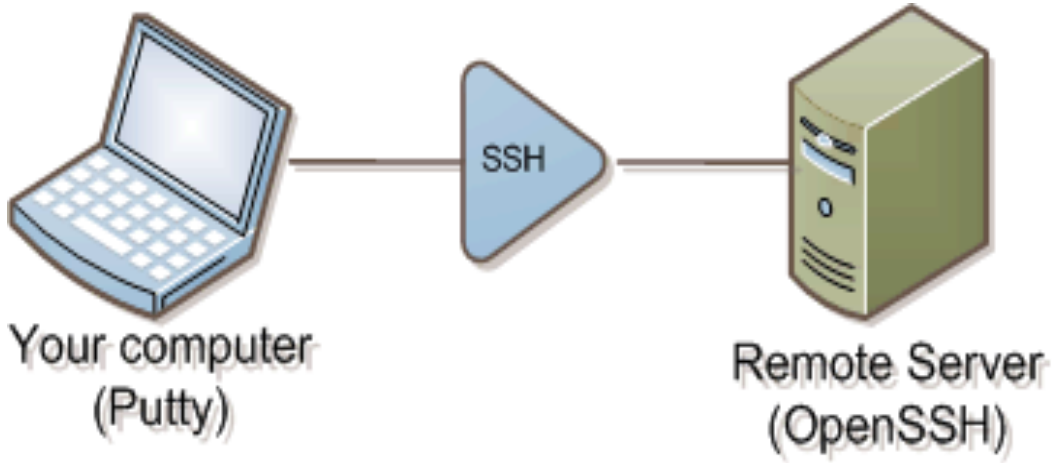
- Management session on top of existing data connection
- Needs L3 connectivity – IP addresses are required
- More convenient to use but not always secure and reliable

Telnet



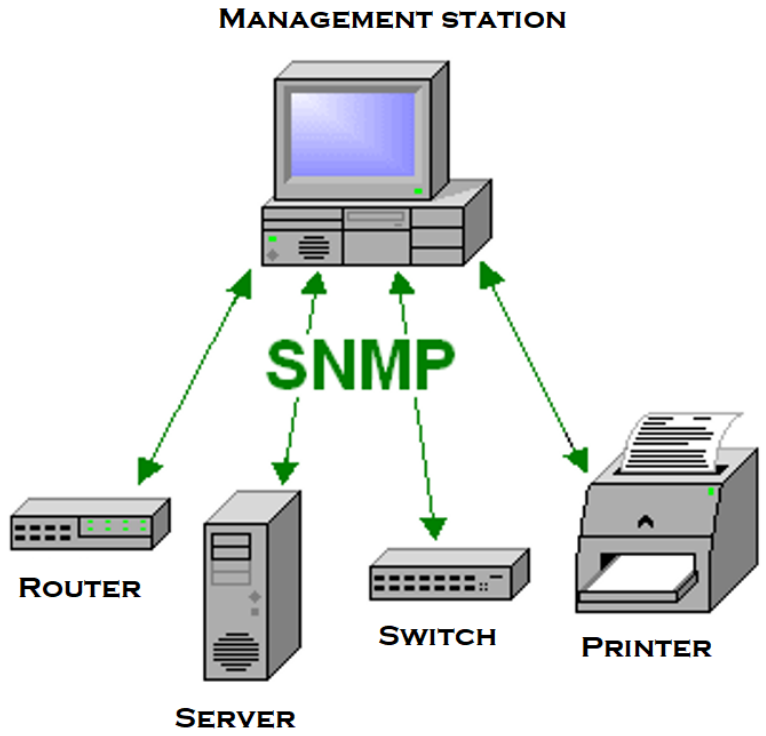
- Common protocol for managing networking devices
- Works on TCP port 23 (by default)
- Low security – does not provide encryption
- Easy to configure and use

SSH (Secure Shell)



- SSH (Secure Shell) – the secure alternative of Telnet
- Uses public-key cryptography to authenticate the remote computer
- Works on TCP port 22 (by default)
- A bit more difficult to setup

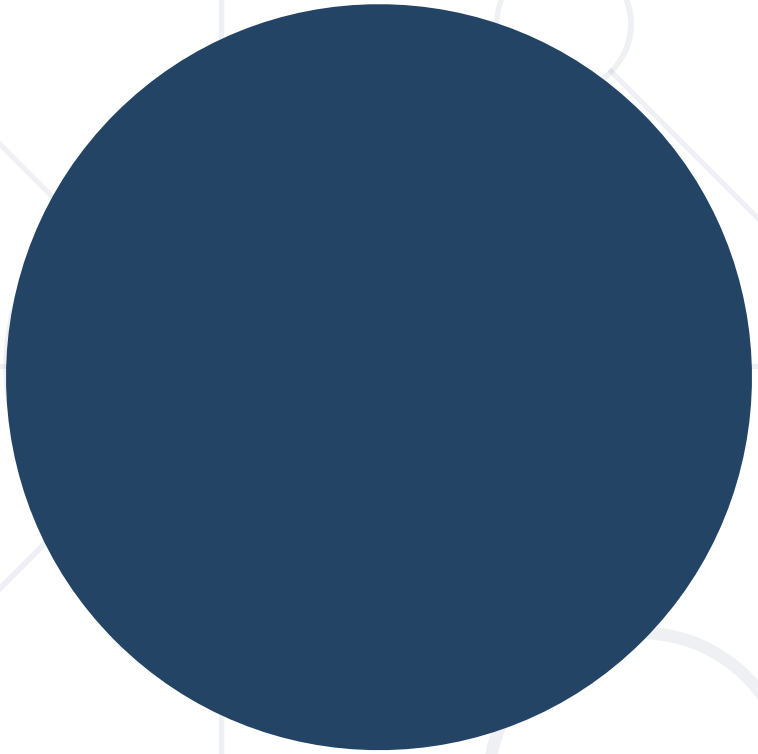
SNMP overview



- SNMP - Simple Network Management Protocol
- Used to collect data about managed devices on an IP network
- Can also be used to push configurations to the devices
- A lot of Network Management Systems use SNMP as their underlying protocol

SNMP Versions

- SNMP v1
  - poor security
  - not very good performance
- SNMP v2c
  - poor security
  - better performance
- SNMP v3
  - Secure and with good performance
  - More difficult to configure



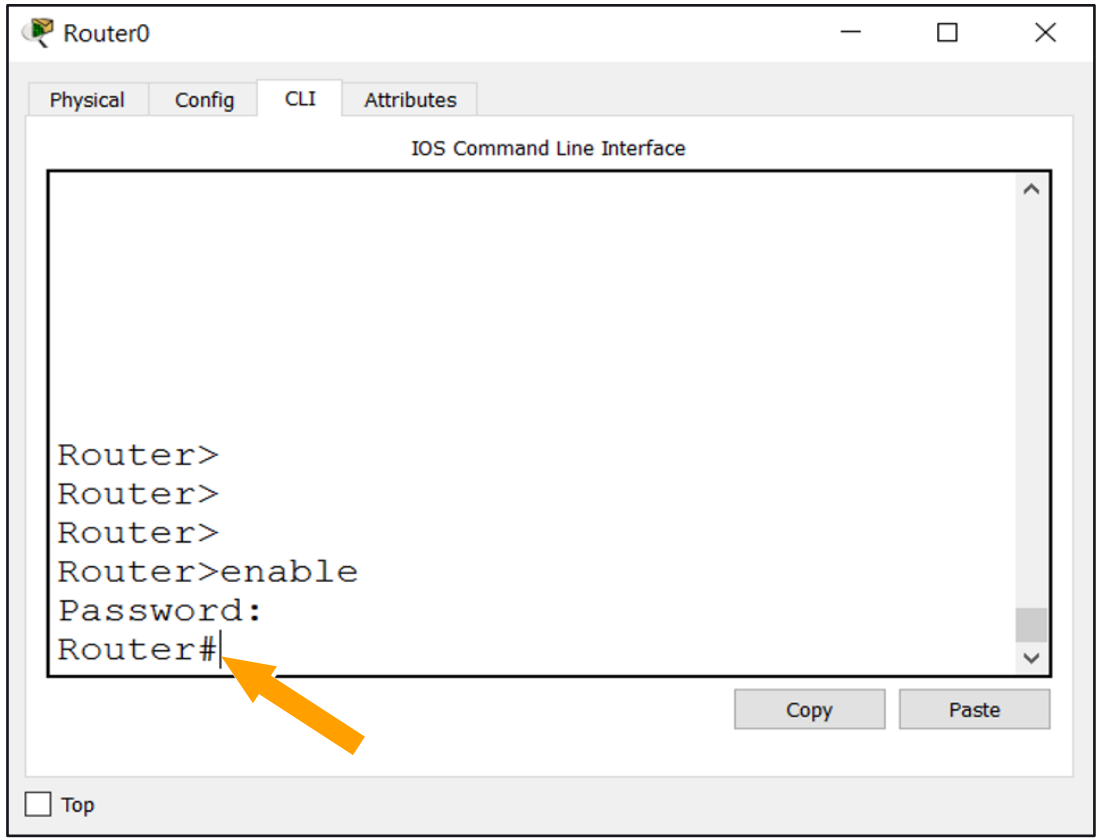
Securing network device access

Where to apply device access security?

- Physical security (often underestimated)
- Set passwords and privileges
- Implement ACLs (will be discussed in the advanced course)

NOTE: Different vendors use different methods for setting and resetting passwords. The next slides will focus on some general Cisco concepts

The enable password/secret



- The password to protect the privilege exec mode (privilege level 15)
- Can be set with either:
  - *enable password*
  - *enable secret*
- Recommended to use enable secret for better security

Interfaces to protect

- Two important interfaces to be protected:
  - **Line Console 0** – the console access (out-of-band)
  - **Line VTY 0 N*** – the Telnet and/or SSH access connections (in-band)

***N** depends on the OS, usually is 15 or 63

Authentication methods

- Each interface (console or VTY) can be configured to:
  - Does not ask for a password: no login
  - Asks for a password: login
  - Asks for a username and password: login local
    (Local accounts must exist to support it)

* These are Non-AAA Authentication methods

Privilege levels

- Two default privilege levels are configured:
  - privilege 1 - this is the user exec mode >
  - privilege 15 - this is the privileged exec mode #
- You can also define custom levels numbered from 2 to 14 and:
  - Associate each level with allowed commands (use the privilege command)
  - Assign a password to level n (enable secret level n password)

Encrypting all passwords

```
service password-encryption
!
hostname Router
!
!
!
enable secret level 5 5 $1$mERr$9qivvjZYjhss745k8JBnF1
enable secret level 10 5 $1$mERr$Wlb6JtQxHD8YGwb3eLG8K0
enable secret 5 $1$mERr$3HhIgMGBA/9qNmgzccuxv0
enable password 7 08701E1D
!
!
!
!
!
 --More--
```

- To encrypt all passwords in the configuration, use the service password-encryption command

Password reset

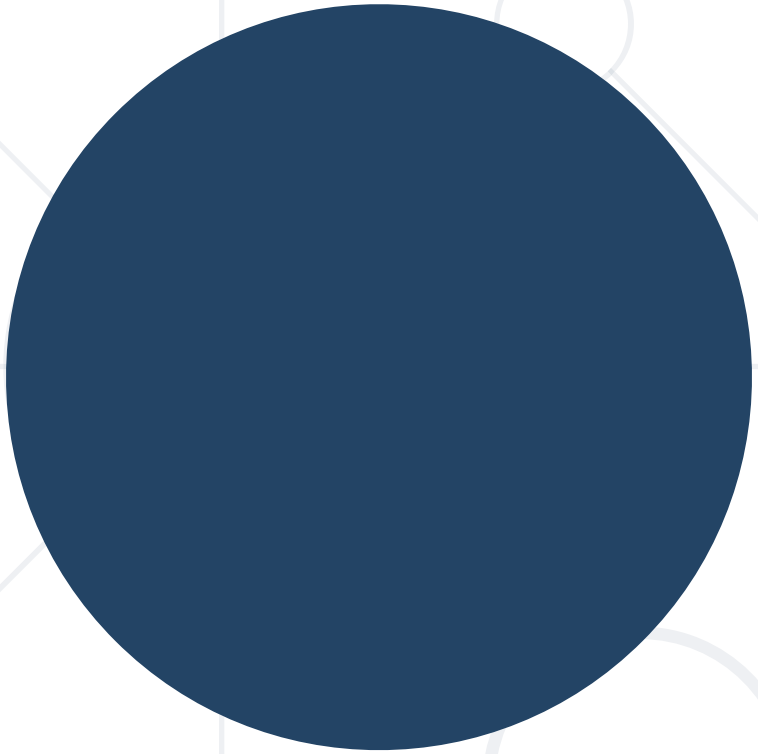
- Lost or forgotten passwords can be reset if you have local access to the device, typically with console connection
- A password is not recovered meaning that you typically can not find the lost one
- Instead, you specify a new password (or delete the old one)

Password reset procedure

1. Enter into the emergency (rommon) mode
2. Instruct the device to bypass its config file (set the configuration register to 0x2142)
3. Load the device without configuration
4. Make “copy start run”
5. Delete the password or configure a new one
6. Save the config
7. Set the configuration register back to 0x2102
8. Reboot

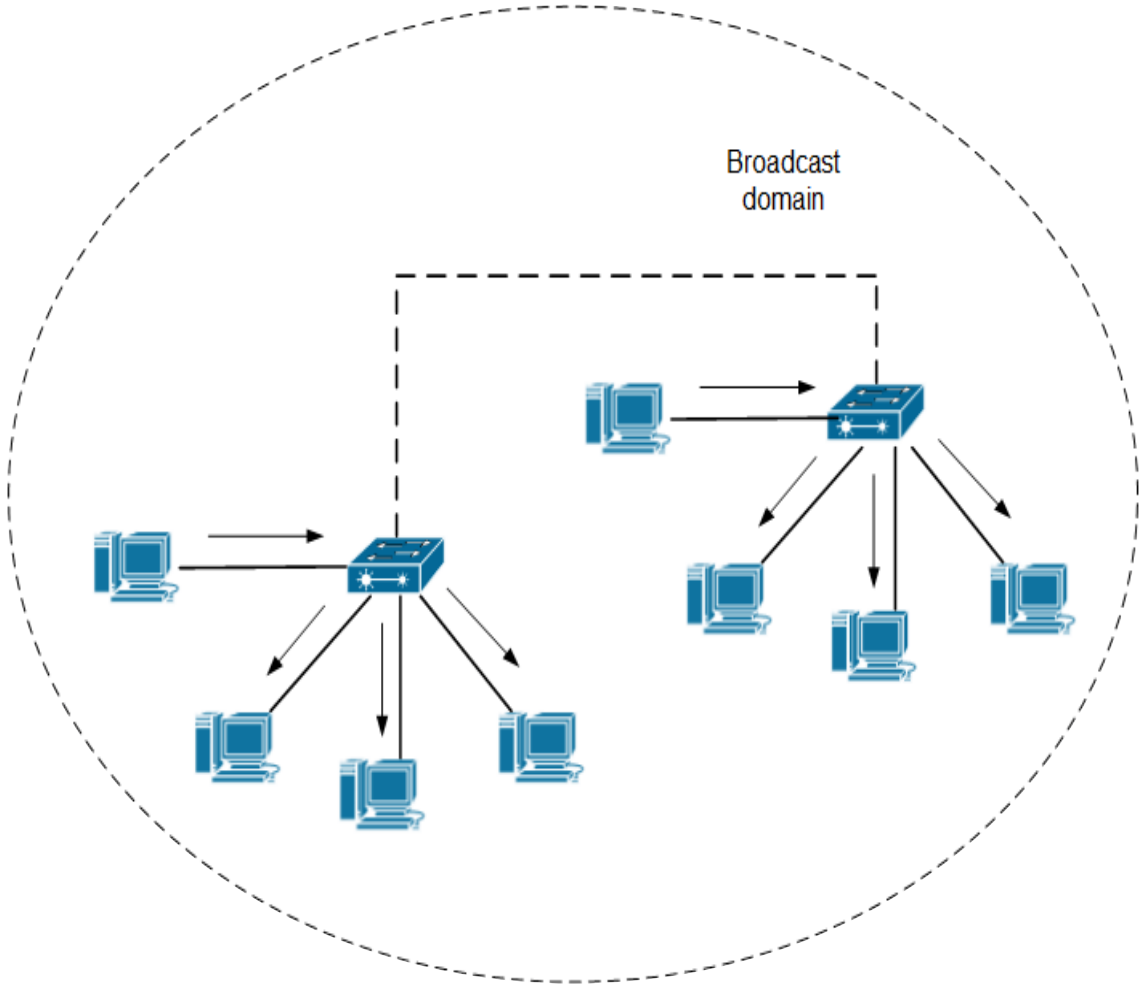
Secure Access - best practices

- Physically secure the devices
- Use SSH instead of Telnet
- Use SNMPv3 instead of v1 or v2
- Use HTTPS instead of HTTP
- Out-of-band management (console) is considered more secure than in-band management
- Create strong passwords for each privilege level and method of access (console, VTY)



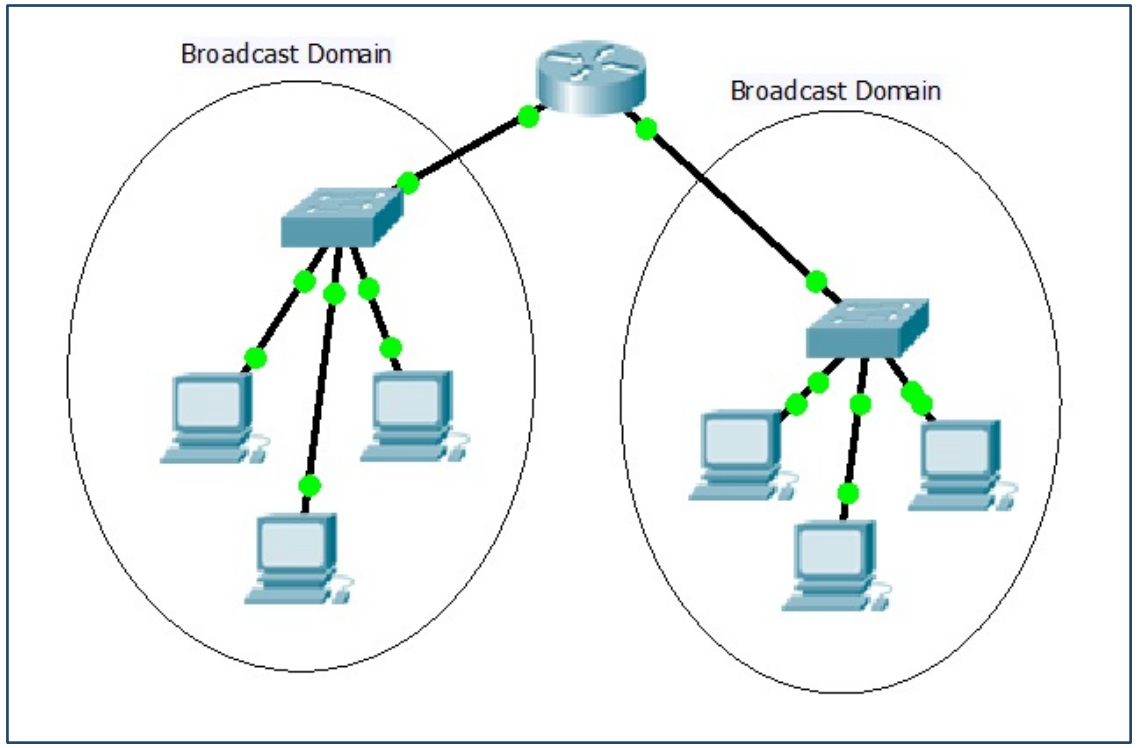
Introduction to VLANs

A network without (V)LANs



- A single LAN with many computers have some drawbacks:
  - Low performance - bigger broadcast domain means less efficient utilization of the links
  - Bad security - each user can configure an IP address from the same network and there is no L2 isolation

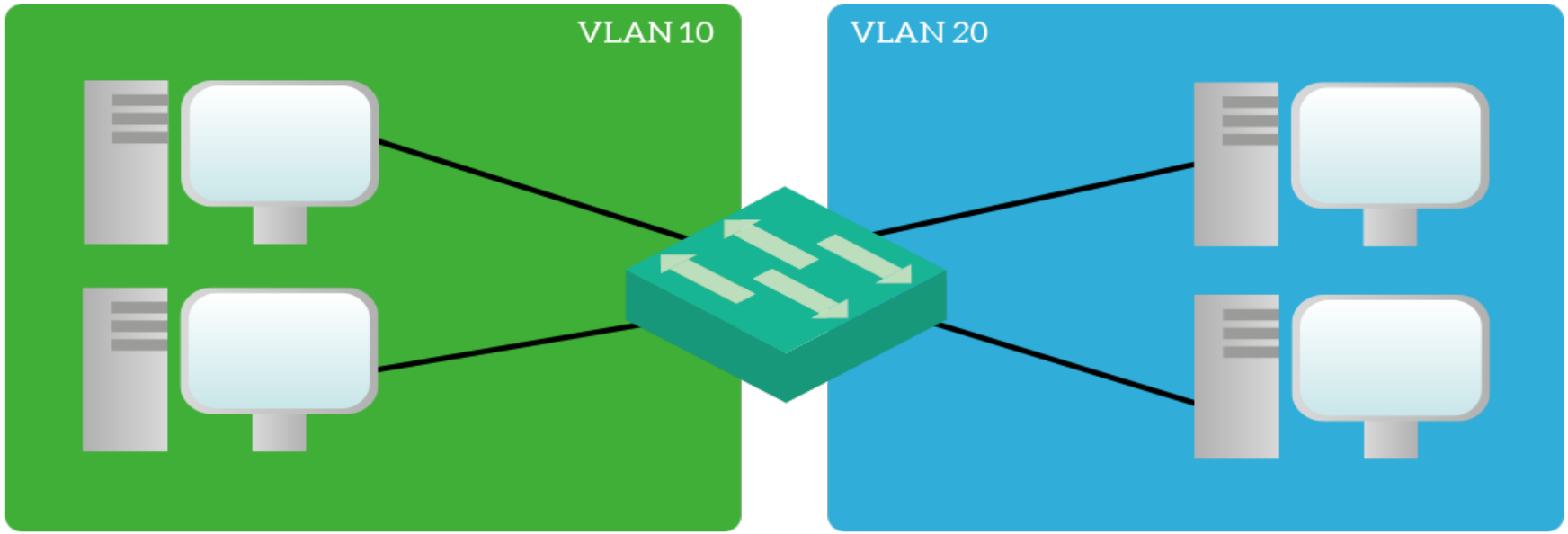
Multiple LANs separated with a router



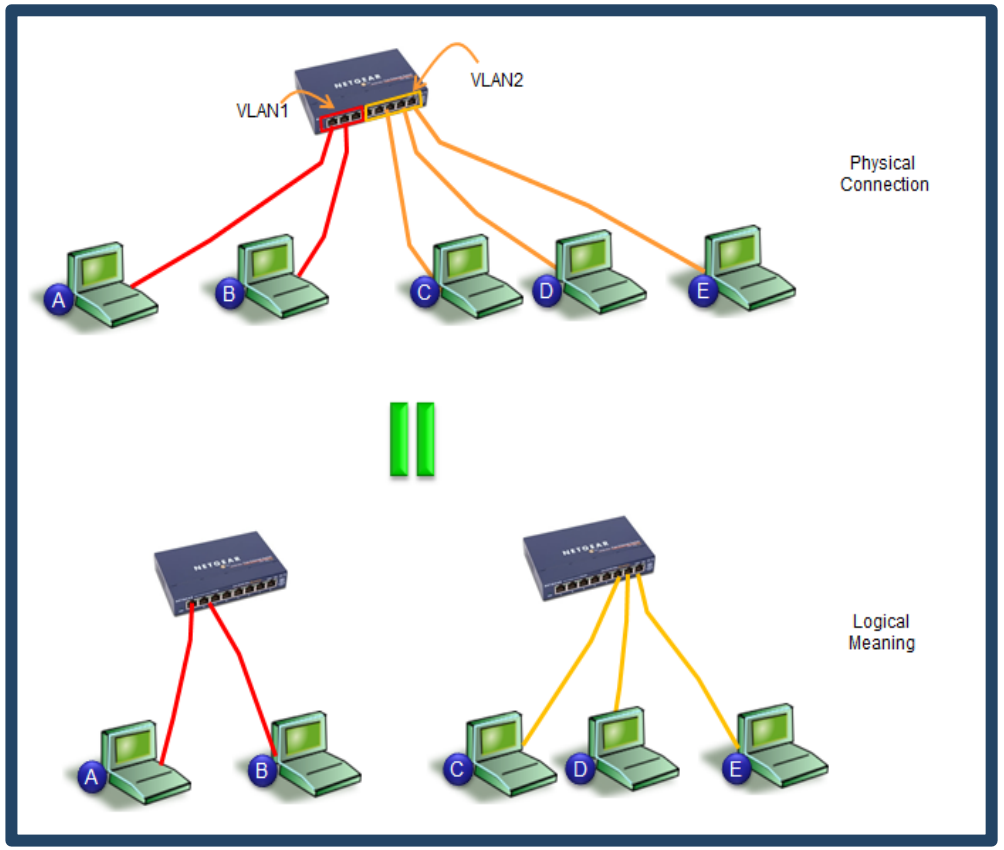
- A router may connect multiple LANs, which provides:
  - better performance (multiple broadcast domains)
  - better security (controlled by the router)

VLANs: Virtual LANs

- Logical division of computer networks
- One VLAN = One broadcast domain
- One VLAN = One IP subnet

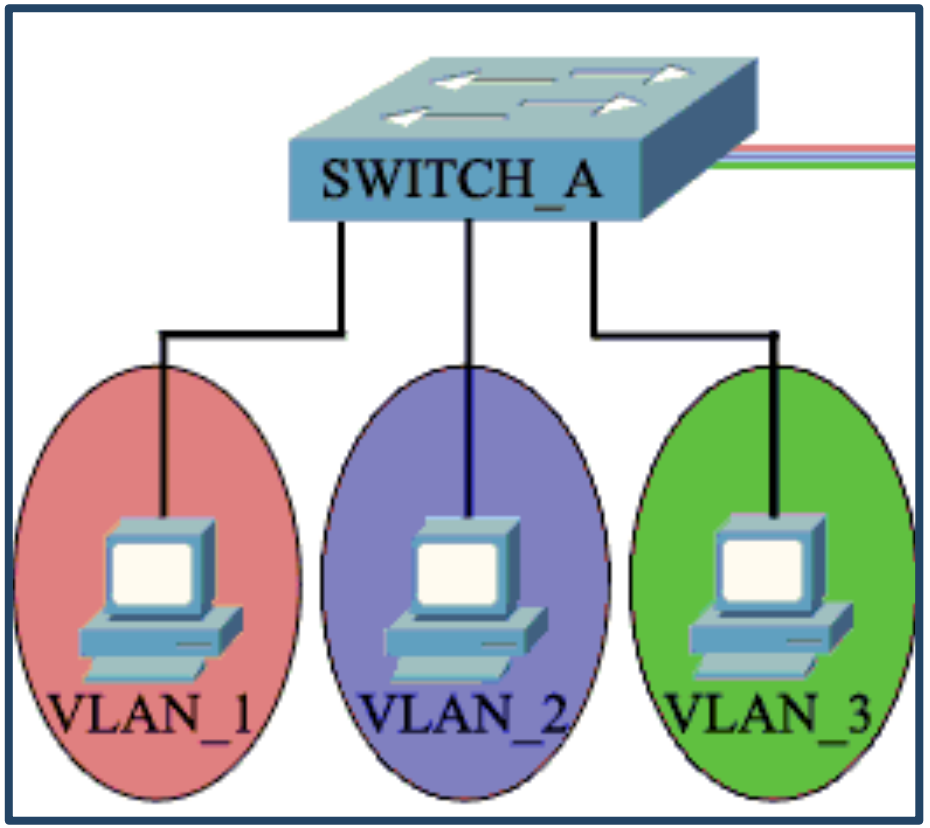


The benefits of the VLANs



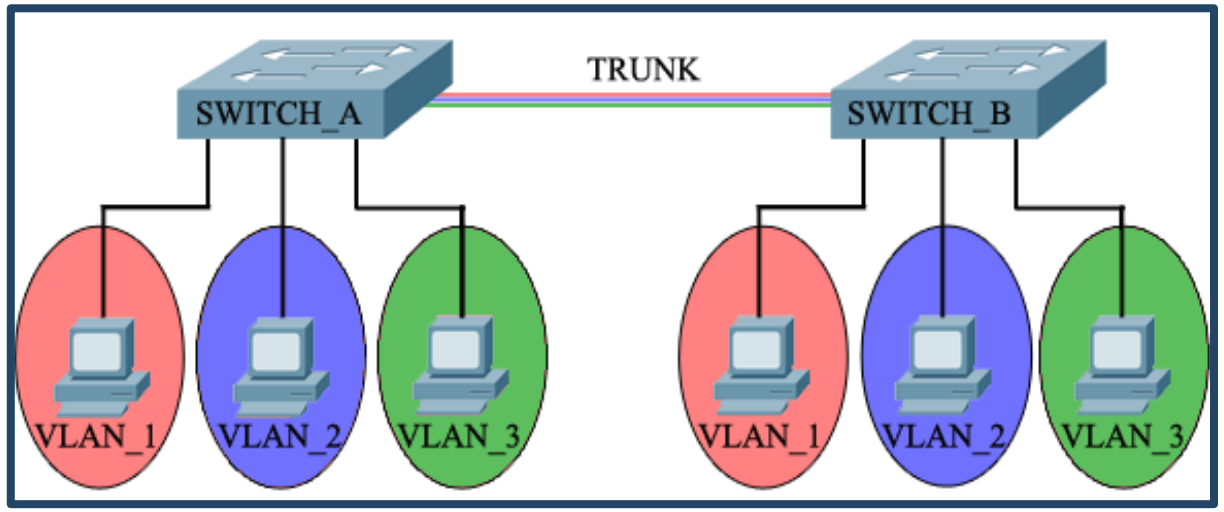
- Better performance (multiple broadcast domains)
- Better security - no connection between the VLANs (unless a L3 device is configured to do this)
- Flexibility - regardless of a user's location, he/she can belong to any VLAN configured by administrator

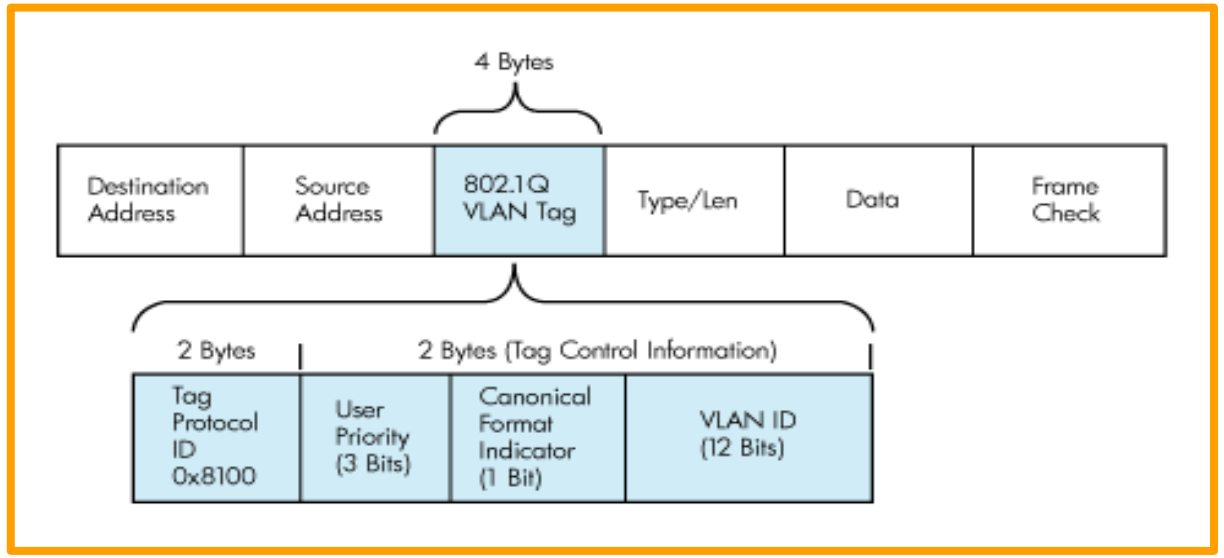
Access (untagged) ports



- Used to connect to end-user devices
- Can be associated with only one VLAN
- Uses the “normal” ethernet frame where there is no VLAN information - no VLAN tag

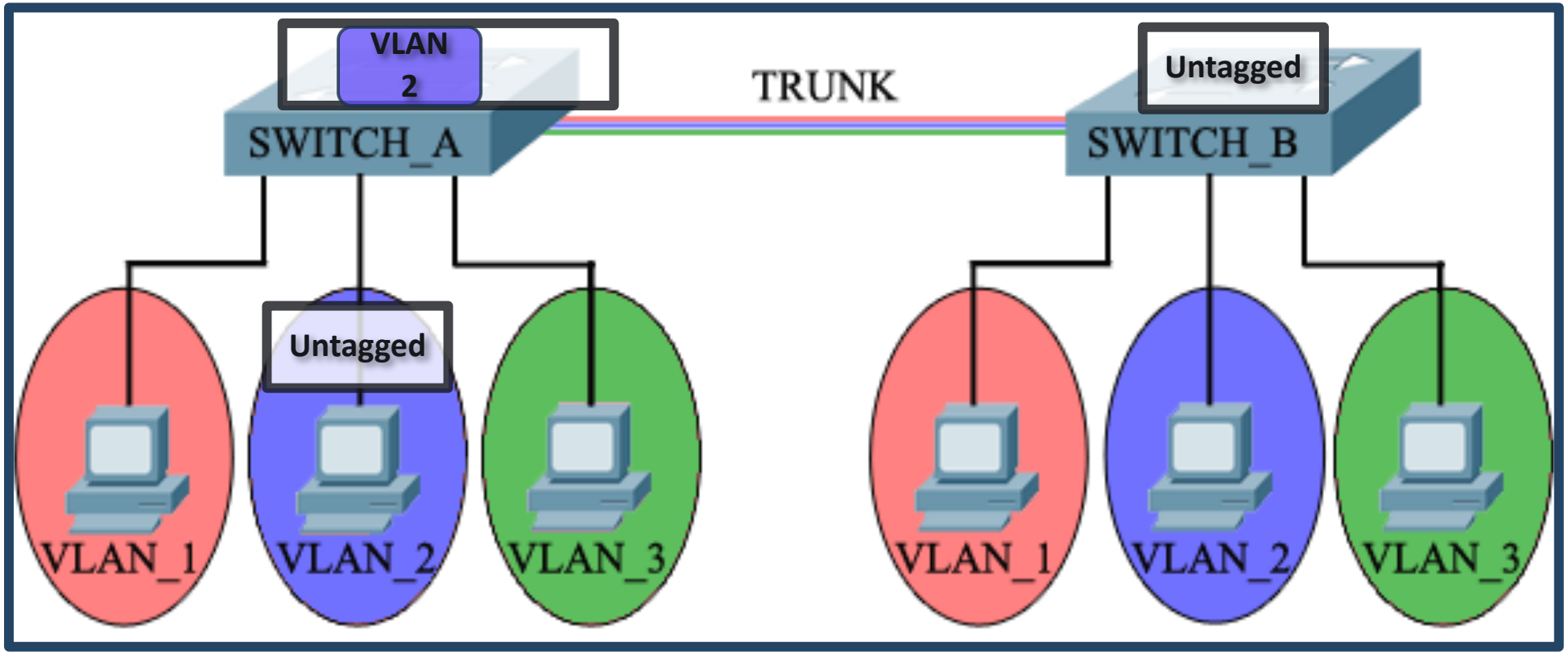
Trunk (tagged) ports

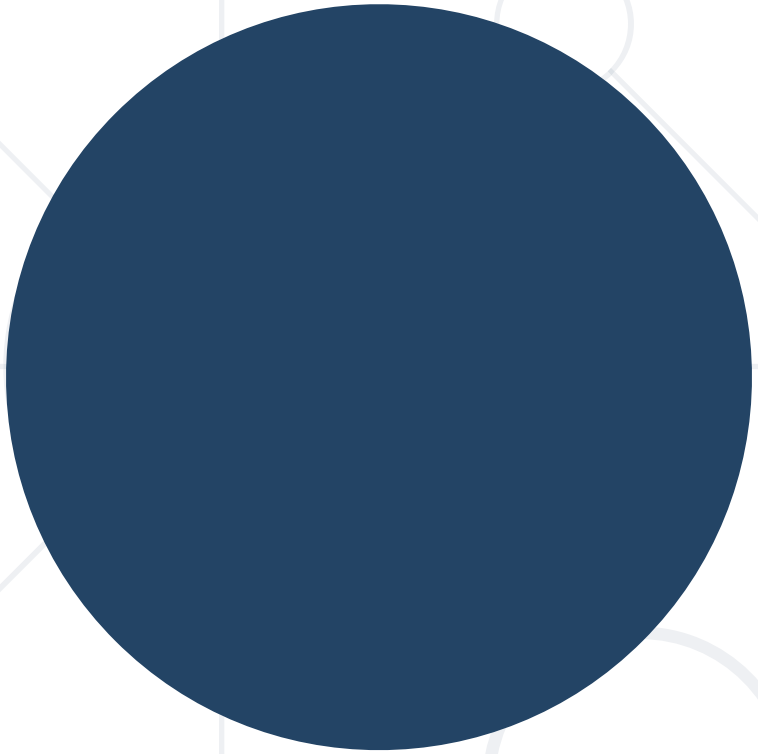




- Used to connect between switches
- Can carry information from/to multiple VLANs
- Uses the 802.1Q tagged frame

Tagging between switches



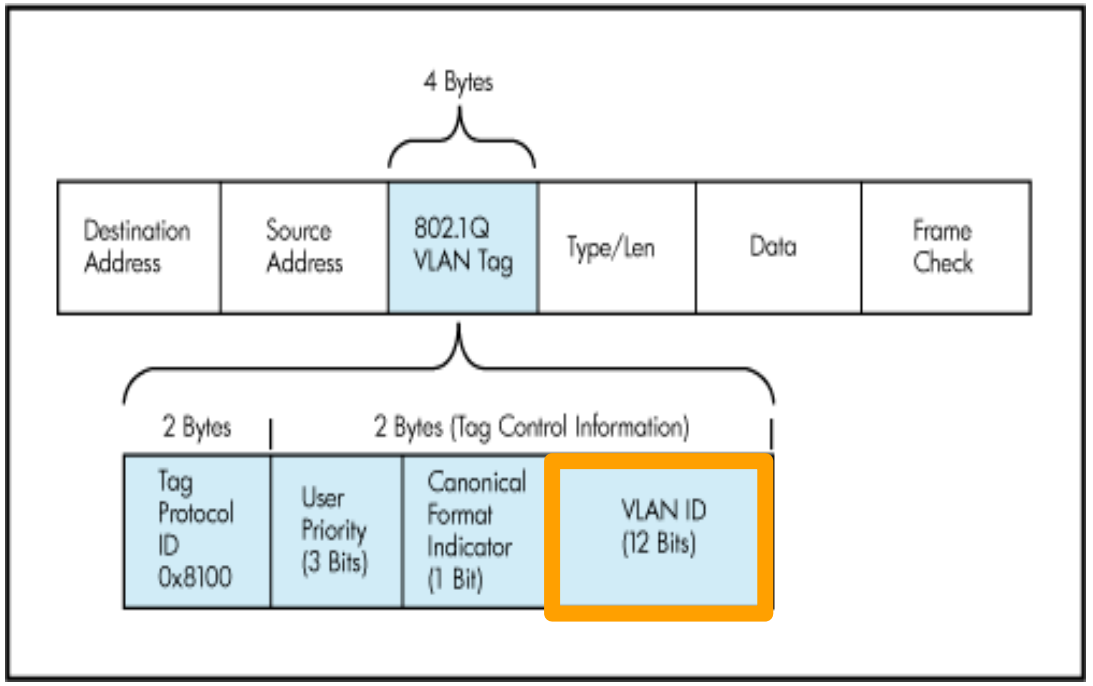


VLAN details

VLANs: defaults and rules

- By default, there is only VLAN 1 in each switch
- By default, ALL ports belong to VLAN 1 untagged (access ports)
- VLAN 1 can not be deleted
- Each port must be member of at least one VLAN
- Untagged port can belong to only one VLAN at a time
- Trunk ports can belong to multiple VLANs at the same time (tagged)

Trunk port details



- Uses IEEE 802.1Q tag to identify each frame
- A trunk carries multiple tagged VLANs and (maximum) one untagged VLAN
- The untagged VLAN on a trunk is called:
  - Native VLAN (Cisco)
  - PVID (HPE Comware)
  - Untagged VLAN (HPE Provision)

Trunk port details (2)

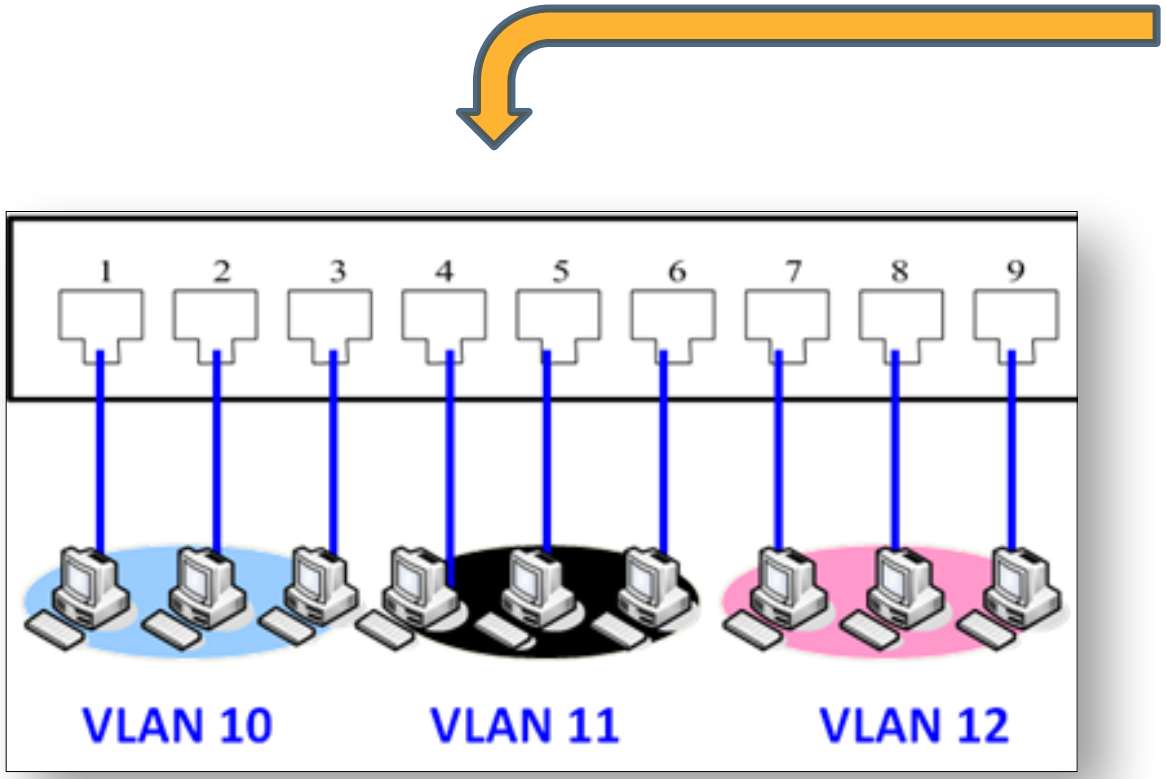
- When a port is configured as a trunk port, different vendors may have different default behavior:
  - All VLANs are automatically allowed on the trunk - Cisco
  - None of the VLANs (except VLAN 1) are auto-allowed on the trunk - HPE Comware

- The configuration can be changed to overwrite the default behavior depending on your needs

Common VLAN terms

- Default VLAN - all ports belong there by default
- Data VLAN - for the end users
- Native VLAN (PVID) - untagged
- Management VLAN - type of out-of-band management
- Voice VLAN - typically has higher priority
- Private VLAN - a.k.a. port isolation

Types of VLANs



- Port based VLANs
- MAC address based VLANs
- IP subnet based VLANs
- Protocol based VLANs
- Others

Inter-VLAN routing

- Traffic is transferred from one VLAN to another via routing
- Layer 3 device with IP address in each VLAN is required
- Do I have Layer 3 support on my switch?
  - Cisco – L3 default state depends on the device
  - HPE Comware - L3 is always on
  - HPE Provision - need to manually turn on the ip routing

Summary

1. Device Memory Components
2. Accessing Network Devices
3. Securing Network Device Access
4. Intro to VLANs
5. VLAN Details