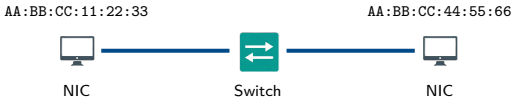
Network Interfaces and Switches

Network+ Module 3.0

Brendan Shea, PhD

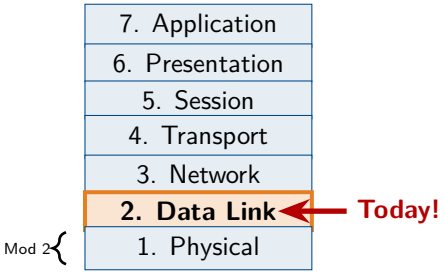
Rochester Community and Technical College
Intro to Networking



Outline I

Review: From Cables to Connections

- Module 2 covered **physical cables**—copper, fiber, and connectors.
- Today's question: What do those cables *plug into*?
- Two key components:
  - **NICs**—in computers (endpoints)
  - **Switches**—connecting everything together
- We're moving from Layer 1 (Physical) into Layer 2 (Data Link).



Layer 2 Focus

Cables carry bits, but NICs and switches work with **frames** and **MAC addresses**.

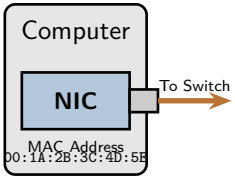
Learning Outcomes I

After completing this module, you will be able to:

- Explain the function of **Network Interface Cards (NICs)** and their role in host connectivity.
- Identify and describe **modular transceivers** including SFP, SFP+, and QSFP.
- Interpret **MAC addresses** and explain the **OUI** (Organizationally Unique Identifier) format.
- Describe the structure of an **Ethernet frame** and identify its key fields.
- Compare and contrast **hubs**, **bridges**, and **switches** as Layer 2 devices.
- Explain how switches use **MAC address tables** to make forwarding decisions.
- Configure basic switch settings including hostnames, IP addresses, and **link aggregation**.
- Describe advanced switch features including **STP**, **PoE**, and Layer 3 switching.
- Troubleshoot common switch problems using LED indicators, **show commands**, and error counters.

What is a Network Interface Card (NIC)?

- A **NIC** is the hardware that connects a computer to the network.
- Every NIC has a unique **MAC address** burned in at the factory.
- NICs translate between computer data and network signals (electrical or optical).
- Modern computers usually have NICs built into the motherboard.



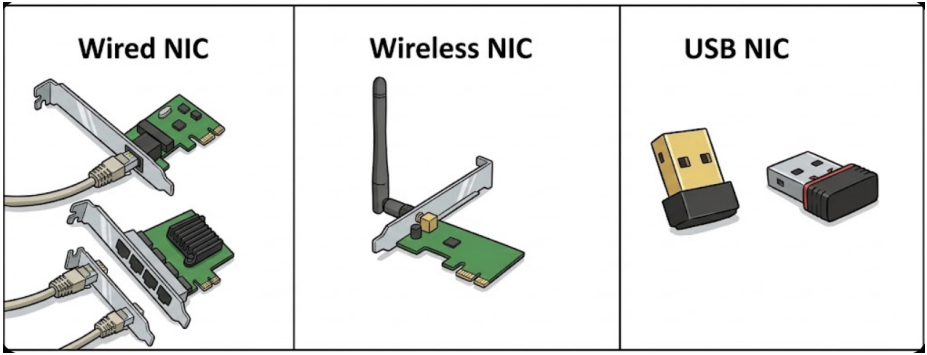
NIC Responsibilities

- Create and process Ethernet frames
- Convert data to/from network signals
- Manage link speed and duplex settings

Key Point

Without a NIC, your computer is an island—no network access!

NIC Examples



Examples of different network interface cards showing various form factors and connector types.

NIC Features and Specifications

- **Speed ratings**: 1 Gbps, 10 Gbps, 25 Gbps, 100 Gbps.
- **Connector types**: RJ-45 (copper) or SFP/SFP+ (fiber).
- **Wake-on-LAN (WoL)**: Start a powered-off computer remotely over the network.
- **Offloading**: NIC handles checksums, segmentation—reduces CPU load.
- Server NICs often have multiple ports.

NIC Type	Typical Use
1 Gbps RJ-45	Desktops, laptops
10 Gbps RJ-45	Workstations
10 Gbps SFP+	Servers
25/100 Gbps	Data centers

Auto-Negotiation

NICs automatically negotiate the best speed and duplex with the switch. Usually "just works"!

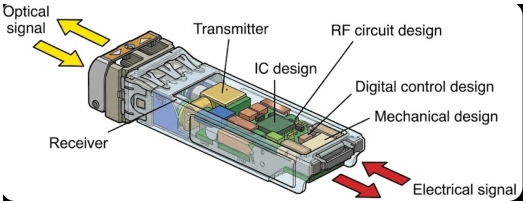
Dual-Port NICs

Servers use multiple NIC ports for:

- Redundancy (failover)
- Increased bandwidth
- Separate networks

What is a Transceiver?

- A **transceiver** is a device that both **transmits** and **receives** signals.
- Converts between electrical signals (inside the device) and optical or electrical signals (on the cable).
- **TX**: Transmit (outgoing signal)
- **RX**: Receive (incoming signal)
- Think of it as a translator between two different "languages" of communication.



Why Transceivers Matter

Without a transceiver, your switch can't understand fiber optic light signals—it only speaks electrical!

Key Components

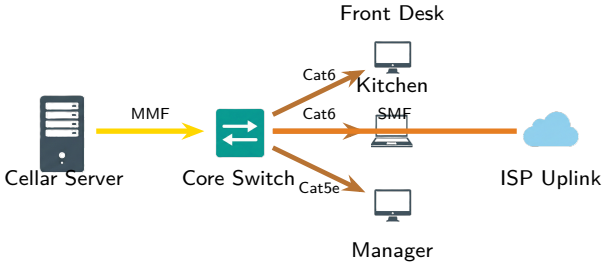
Laser/LED: Converts electrical → light
Photodetector: Converts light → electrical
Circuit board: Manages the conversion

Table: Types of Transceivers

Transceiver	Speed	Cable Type	Connector	Distance
SFP	1 Gbps	MMF or SMF	LC	550m (MMF) 10km (SMF)
SFP+	10 Gbps	MMF or SMF	LC	300m (MMF) 10–80km (SMF)
QSFP	40 Gbps	MMF or SMF	MPO/MTP	100m (MMF) 10km (SMF)
QSFP28	100 Gbps	MMF or SMF	MPO/MTP	100m (MMF) 10km (SMF)
GBIC (legacy)	1 Gbps	MMF or SMF	SC	550m (MMF) 10km (SMF)
SFP-T	1 Gbps	Copper (UTP)	RJ-45	100m
SFP+ DAC	10 Gbps	Twinax copper	Integrated	3–7m

MMF = Multimode Fiber **SMF** = Single-mode Fiber **DAC** = Direct Attach Cable.
Always match transceiver type to cable type and required distance.

Layer 1: Physical Infrastructure at the Green Dragon



Layer 1 maps physical links between endpoints, switching infrastructure, and uplinks.

Transceiver Issues

Mismatch Issues

- SFP in SFP+ port: May work at reduced speed
- SFP+ in SFP port: **Won't work**
- Different vendors may be incompatible (some switches are picky!)
- Fiber type mismatch: MMF transceiver + SMF cable = no link

Vendor Lock-In

Some manufacturers only accept their own branded transceivers. Third-party modules are cheaper but may not work.

Signal Strength Issues

- **TX power**: How strong the transmit signal is
- **RX sensitivity**: Minimum signal the receiver can detect
- Too little power = signal doesn't reach
- Too much power = overwhelms receiver

Troubleshooting Tip: Transceivers

1. Transceiver compatibility
2. Fiber type (MMF vs SMF)
3. Cable distance vs. transceiver rating

Ethernet Frame Format

- Data doesn't travel as raw bits—it's packaged into **frames**.
- Frames contain addressing information so switches know where to send them.
- Standard maximum frame size: **1518 bytes** (or 9000+ for jumbo frames).

Header Fields

Preamble: Synchronization bits
Dest/Src MAC: Who it's going to/from
Type: What protocol is inside

Trailer Field

FCS (Frame Check Sequence): Error detection—receiver recalculates to verify frame wasn't corrupted.

MAC Address Format

- **MAC (Media Access Control)** address: The hardware address of a NIC.
- 48 bits (6 bytes), written in hexadecimal.
- Also called: physical address, hardware address, or **burned-in address (BIA)**.
- Every NIC has a unique MAC assigned by the manufacturer.
- Operates at **Layer 2** (Data Link) of the OSI model.

Common Formats

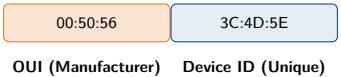
`00:1A:2B:3C:4D:5E` (colons)
`00-1A-2B-3C-4D-5E` (dashes)
`001A.2B3C.4D5E` (dots—Cisco)

MAC vs IP

MAC = permanent hardware address (Layer 2).
IP = changeable logical address (Layer 3).

MAC Address Deep Dive

- First 3 bytes: **OUI (Organizationally Unique Identifier)**—identifies the manufacturer.
- Last 3 bytes: **Device ID**—unique to each NIC from that manufacturer.
- OUIs are assigned by IEEE—you can look them up online!



Example OUIs

`00:50:56` = VMware
`00:0C:29` = VMware (alternate)
`00:1A:A0` = Dell

Special MAC Addresses

Broadcast: `FF:FF:FF:FF:FF:FF`
Goes to ALL devices on the network.

Multicast: Starts with `01:00:5E`
Goes to a group of devices.

Can MACs Be Changed?

Yes! Software can "spoof" a different MAC. Useful for troubleshooting, but also a security concern.

Case Study: Sam's First NIC Installation

▶ Case Study: Sam's First NIC Installation

Samwise Gamgee is setting up the new admin burrow network for the Shire. He purchases 10 Gbps NICs for the hobbit-hole workstations, but the switches only have SFP ports (1 Gbps, not SFP+).

Sam also notices one workstation showing a MAC address of `00:00:00:00:00:00` in the network settings.

Review Questions

1. Will the 10 Gbps NICs work in the 1 Gbps switch ports?
2. What speed will the connection actually operate at?
3. What might cause a MAC address of all zeros?

Case Study Solution: Sam's First NIC Installation

✓ Solution: Sam's First NIC Installation

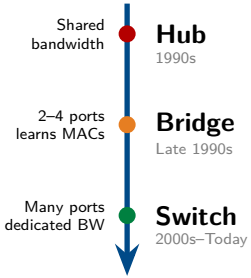
1. **Yes**—10 Gbps NICs will auto-negotiate down to match the switch's 1 Gbps capability.
2. The connection will operate at **1 Gbps**—limited by the slower device (the switch).
3. All-zeros MAC address typically means:
   - NIC driver not installed or loaded
   - NIC hardware failure
   - Virtual/unconfigured network adapter

Key Lessons

- Always match NIC and switch capabilities for best performance—Sam could save money using 1G NICs.
- A missing or abnormal MAC address points to driver or hardware problems.

The Evolution: Why Switches?

- Early networks used **hubs**—cheap but problematic.
- Then came **bridges**—smarter, but limited ports.
- Now we use **switches**—best of both worlds.
- Understanding this evolution helps you troubleshoot legacy networks.

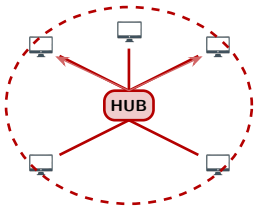


The Core Problem

How do we connect multiple devices efficiently without wasting bandwidth or causing collisions?

Hubs: Shared Bandwidth (and Problems)

- A **hub** repeats every signal to **every port**.
- Like shouting in a room—everyone hears everything.
- All devices share the same **collision domain**.
- Only **half-duplex** communication possible.
- More devices = more collisions = worse performance.



1 Collision Domain

Why Hubs Are Obsolete

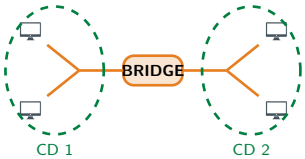
10 devices on a 100 Mbps hub = roughly 10 Mbps each (minus collision overhead). Terrible!

Hub = Layer 1

Hubs operate at the Physical layer—they don't understand MAC addresses.

Bridges: Learning MAC Addresses

- A **bridge** learns which devices are on which side.
- Maintains a **MAC address table**.
- Only forwards traffic that needs to cross.
- Separates **collision domains**—fewer collisions!
- Limited to 2–4 ports (not scalable).



Bridge = Layer 2

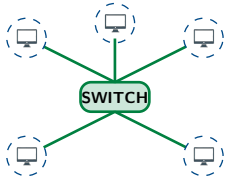
Bridges read MAC addresses and make forwarding decisions—smarter than hubs!

Selective Forwarding

Traffic between L1 and L2 stays on the left—the bridge doesn't forward it right.

Switches: The Modern Solution

- A **switch** is essentially a multi-port bridge.
- Each port is its own **collision domain**—no collisions!
- **Full-duplex** communication on every port.
- **Dedicated bandwidth** per port (not shared).
- Learns MAC addresses automatically.



5 Collision Domains

Bandwidth Advantage

A 24-port Gigabit switch = up to 24 Gbps total capacity (each port gets full 1 Gbps).

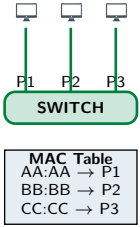
Switch = Layer 2

Like bridges, switches read MAC addresses—but with many more ports and better performance.

How Switches Learn and Forward

The Four Switch Actions

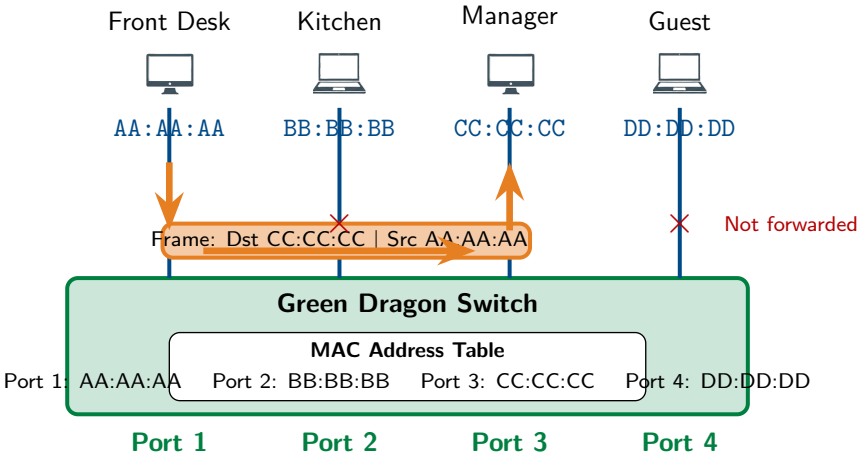
1. **Learning**: See source MAC → record which port it came from
2. **Forwarding**: Know destination MAC → send only to that port
3. **Flooding**: Unknown destination → send to ALL ports (except source)
4. **Filtering**: Same-segment traffic → don't forward



MAC Address Table

The switch builds a table mapping MAC addresses to ports. This is how it knows "who is where."

Layer 2: MAC Address Communication at the Green Dragon



Layer 2 uses **MAC addresses** to forward frames. The switch sends traffic **only to the destination port**—not everywhere.

Unmanaged vs Managed Switches

Unmanaged Switch

- Plug and play—no configuration
- No VLANs, no monitoring
- Cheapest option
- Best for: Home, very small office

Managed Switch

- Full configuration options
- VLANs, STP, SNMP, port security
- CLI, web GUI, remote management
- Best for: Enterprise networks

Smart Switch

- Some management features
- Basic VLANs, simple web GUI
- Middle price range
- Best for: Small business

Key Question

Do you need to separate traffic, monitor performance, or configure security? If yes $\rightarrow$ managed switch.

Layer 2 vs Layer 3 Switches

Layer 2 Switch (Standard)

- Forwards based on **MAC addresses**
- Cannot route between networks
- Needs a router for inter-VLAN traffic
- Less expensive

Layer 3 Switch (Multilayer)

- Also routes based on **IP addresses**
- Can route between VLANs directly
- Faster than using separate router
- More expensive

Routes internally!

When to Use Layer 3 Switches

Large networks with multiple VLANs benefit from Layer 3 switches—inter-VLAN traffic stays fast without bottlenecking through a router.

Switch Interface Configuration Basics

Access Methods

- **Console cable**: Direct serial connection (initial setup)
- **SSH/Telnet**: Remote CLI over network
- **Web GUI**: Browser-based (some models)

Common Settings

- Port speed (10/100/1000)
- Duplex mode (half/full/auto)
- VLAN assignment
- Port description/label

Speed/Duplex Mismatch

If one side is set to auto and the other is manually configured, they may negotiate incorrectly. Result: slow speeds, errors, packet loss.

Port Security

Limit which MAC addresses can connect to a port:

- Prevent unauthorized devices
- Protect against MAC flooding attacks
- Can shut down port on violation

Case Study: The Green Dragon Inn Network

▶ Case Study: The Green Dragon Inn Network

The Green Dragon Inn is expanding and needs a network for guest hobbits and staff. Frodo suggests a cheap unmanaged switch. Gandalf recommends a managed switch instead.

The network requirements:

- Separate guest traffic from staff traffic (security)
- Support 20 devices total
- Allow remote management (Gandalf travels frequently)

Review Questions

1. Which switch type should they choose and why?
2. What feature would separate guest from staff traffic?
3. Why is remote management valuable for an inn?

Case Study Solution: The Green Dragon Inn Network

✓ Solution: The Green Dragon Inn Network

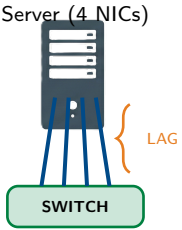
1. **Managed switch**—unmanaged switches cannot separate traffic or be configured remotely.
2. **VLANs (Virtual LANs)** separate guest and staff traffic logically on the same physical switch.
3. Remote management benefits:
   - Gandalf can troubleshoot from anywhere in Middle-earth
   - Monitor bandwidth usage and detect problems
   - Make changes without disrupting inn operations

Key Lesson

The extra cost of managed switches pays off in flexibility and security. For any business network, managed is the right choice.

Link Aggregation and NIC Teaming

- Problem: One cable isn't fast enough for a busy server.
- Solution: Bundle multiple cables together!
- **Link Aggregation (LAG)**: Combines switch ports into one logical link.
- **LACP (802.3ad)**: Protocol that negotiates aggregation automatically.
- **NIC Teaming**: Same concept on the server side.



Benefits

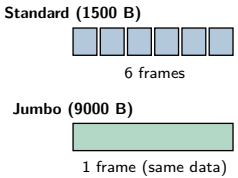
More bandwidth: $4 \times 1\text{G} = 4$ Gbps total
Redundancy: If one link fails, others continue

Both Ends Must Match

LAG must be configured on both the switch AND the server/other switch.

Maximum Transmission Unit (MTU)

- **MTU**: Maximum frame payload size a network can handle.
- Standard Ethernet MTU: **1500 bytes**.
- **Jumbo frames**: MTU up to **9000 bytes**—more efficient for large transfers.
- Larger frames = fewer frames = less overhead.



Critical Requirement

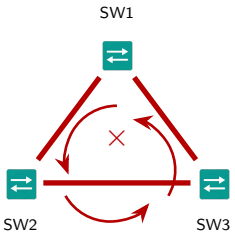
Every device in the path must support the same MTU! Mismatched MTU causes fragmentation or dropped packets.

When to Use Jumbo Frames

- Storage networks (iSCSI, NFS)
- Backup systems
- Data center internal traffic

Spanning Tree Protocol: The Problem

- What happens if you create a **loop** in a switched network?
- Frames have no TTL (time-to-live) at Layer 2—they circulate forever!
- Result: **Broadcast storm**—frames multiply exponentially.
- Network grinds to a halt in seconds.
- Loops happen accidentally (wrong cable) or intentionally (redundancy gone wrong).



Real Danger

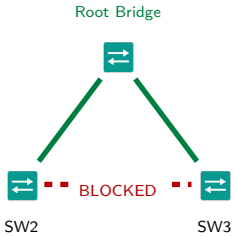
An accidental loop can crash an entire network in under 30 seconds!

Symptoms

All switch LEDs flashing rapidly, network unresponsive, high CPU on switches.

Spanning Tree Protocol: The Solution

- **STP (802.1D)** automatically detects and blocks redundant paths.
- Elects a **root bridge**—the central reference point.
- Calculates best path from each switch to the root.
- **Blocks** redundant ports to prevent loops.
- If active link fails, blocked port activates—redundancy preserved!



STP Versions

802.1D (STP): Original, slow (30–50 sec)
802.1w (RSTP): Rapid, fast (1–2 sec)
802.1s (MSTP): Per-VLAN spanning trees

Key Insight

STP provides redundancy WITHOUT loops—blocked ports wait as backups.

Power over Ethernet (PoE)

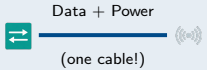
- **PoE** delivers electrical power AND data over the same Ethernet cable.
- No separate power outlet needed at the device!
- Perfect for: IP phones, security cameras, wireless access points, IoT devices.
- Switch must be **PoE-capable** or use a separate **PoE injector**.

Standard	Power	Devices
802.3af	15.4W	IP phones
802.3at (PoE+)	30W	Cameras, APs
802.3bt (PoE++)	60–100W	PTZ cameras

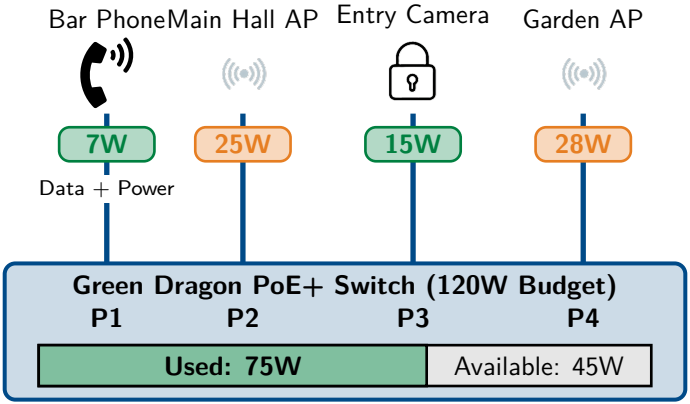
Power Budget

Switches have a total PoE power budget (e.g., 370W). Plan carefully—you can't power unlimited devices!

PoE Advantage



Power over Ethernet: Green Dragon Power Budget



PoE delivers **data and power** over one cable. Always track your **power budget**—the switch has limits!

Case Study: Bilbo's Birthday Party Network Disaster

▶ Case Study: Bilbo's Birthday Party Network Disaster

Bilbo is hosting his 111th birthday party and needs a network for the event planners. Shortly after setup, the entire network crashes—all switches show frantically blinking lights, and no device can communicate.

Merry investigates and discovers someone connected both ends of a patch cable to the same switch to "make the cables neater."

Review Questions

1. What has happened to the network?
2. What protocol should have prevented this?
3. What should they check on the switches?

Case Study Solution: Bilbo's Birthday Party Network Disaster

✓ Solution: Bilbo's Birthday Party Network Disaster

1. A **switching loop** caused a **broadcast storm**—frames multiplied until they overwhelmed every switch.
2. **Spanning Tree Protocol (STP)** should block redundant paths automatically.
3. Immediate actions:
   - Remove the looped cable immediately
   - Check if STP is enabled on all switches
   - Verify switches are managed (unmanaged switches may lack STP)

Key Lesson

Always use managed switches with STP enabled for any business network. A single accidental loop can take down everything!

Hardware Failure and Port Status Indicators

LED Indicators

- **Solid green**: Link up, connected
- **Flashing green**: Active traffic
- **Amber/Orange**: Error or disabled
- **Off**: No link detected

First Troubleshooting Step

Always look at the lights! LEDs tell you port status instantly without logging in.

Common Hardware Failures

- Bad switch port (try another port)
- Failed transceiver module
- Power supply issues
- Overheating (check fans, vents)
- Failed backplane (multiple ports down)

No Link Light?

Check in order: cable $\rightarrow$ NIC $\rightarrow$ switch port $\rightarrow$ transceiver (if applicable).

Switch Show Commands

Essential Commands

`show interfaces`
Port status, speed, duplex, errors

`show mac address-table`
Which MACs learned on which ports

`show spanning-tree`
STP status, root bridge, blocked ports

`show power inline`
PoE status and power consumption

Example Output

```
Switch# show interfaces Gi0/1
GigabitEthernet0/1 is up
  Speed:  1000 Mbps, Duplex:  Full
  Input errors:  0, CRC: 0
  Output errors:  0, Collisions:  0
```

Key Insight

These commands work on Cisco and many other managed switches. Learn them once, use them everywhere.

Interface Error Counters

Error Types

CRC errors: Damaged frames—bad cable, NIC, or interference.

Collisions: Duplex mismatch or hub in path.

Runts: Frames too small (<64 bytes)—collision fragments.

Giants: Frames too large—MTU mismatch.

Input/Output Errors

Input errors: Problems receiving frames.

Output errors: Problems sending frames.

Discards: Frames dropped (buffer full, policy).

Interpretation

A few errors = normal.
Rapidly increasing = active problem!

Pro Tip

Clear counters, wait 5 minutes, check again. If errors accumulate quickly, investigate that port.

MAC Address Table Troubleshooting

- The **MAC address table** shows which devices the switch has learned.
- Use it to verify: Is the device connected? Which port?
- If a MAC appears on the wrong port—cable may be in wrong jack.
- If a MAC is missing—device may be off, disconnected, or NIC failed.

Command

```
show mac address-table
```

Example Output

```
VLAN    MAC Address       Port
--    ------       --
1      00:1A:2B:3C:4D:5E   Gi0/1
1      00:50:56:AA:BB:CC   Gi0/2
1      FF:FF:FF:FF:FF:FF   CPU
```

MAC Flapping

Same MAC appearing on multiple ports rapidly = possible loop or duplicate MAC address.

PoE Troubleshooting

Common PoE Issues

- Device not powering on
- Insufficient power budget
- Wrong PoE class negotiated
- Cable quality problems

Troubleshooting Steps

1. Verify switch supports PoE
2. Check total power budget remaining
3. Verify cable uses all 4 pairs
4. Check device PoE class requirements
5. Try known-good cable and port

PoE Class	Max Power
Class 0	15.4W (default)
Class 1	4.0W
Class 2	7.0W
Class 3	15.4W
Class 4	30W (PoE+)

Cable Matters!

PoE requires all 4 pairs. A cable that "works for data" may fail for PoE if pairs are damaged.

Module 3.0 Summary I

Key Concepts:

- **NIC** (Network Interface Card) connects hosts to networks. Each NIC has a unique 48-bit **MAC address**.
- MAC address format: first 24 bits = **OUI** (vendor ID), last 24 bits = device-specific.
- **Transceivers**: **SFP** (1 Gbps), **SFP+** (10 Gbps), **QSFP** (40 Gbps) provide modular connectivity.
- **Ethernet frame**: Headers include destination MAC, source MAC, and Type/Length. Trailer has FCS for error detection.
- **Hub** (repeater) vs **Bridge** (2-port switch) vs **Switch** (multi-port bridge with MAC learning).
- Switches forward frames based on destination MAC, flooding only to unknown addresses or broadcasts.

Module 3.0 Summary II

Configuration & Troubleshooting:

- **Managed switches**: VLANs, port security, SNMP monitoring. **Layer 3 switches** add routing capability.
- **Link aggregation** (LACP) bundles links for higher bandwidth and redundancy.
- **STP** (Spanning Tree Protocol) prevents Layer 2 loops automatically.
- **PoE** (Power over Ethernet) delivers power to devices like phones and APs over Ethernet cables.
- Troubleshooting: Check LED indicators, use `show` commands, monitor error counters, watch for broadcast storms.