Module 8: Network Operations

Maintaining the Swamp (Network+)

Brendan Shea, PhD

Rochester Community and Technical College

Outline I

Review: Application Services and Resilience

Key Module 7 Ideas

- Application protocols provide web, file, email, and voice services.
- Secure protocols (such as HTTPS and secure file transfer) protect data in transit.
- High availability relies on redundancy and failover planning.

Why This Matters in Module 8

Operations and monitoring keep those services healthy, measurable, and recoverable in production.

Learning Outcomes I

After completing this module, you will be able to:

- Distinguish between **physical diagrams** (racks, cables, ports) and **logical diagrams** (IPs, VLANs, subnets) for network documentation.
- Explain **configuration management** practices including standardized naming conventions, configuration backups, and change control procedures.
- Describe the **network device lifecycle**: procurement, deployment, maintenance, end-of-life (EoL) planning, and disposal.
- Define **baselines** for network performance (bandwidth utilization, latency, packet loss) and explain how they enable anomaly detection.
- Configure **IPAM** (IP Address Management) to track IP assignments, detect conflicts, and manage DHCP/DNS integration.
- Compare device discovery protocols: **CDP** (Cisco proprietary) and **LLDP** (vendor-neutral standard) for topology mapping.

Learning Outcomes II

- Explain **SNMP** (Simple Network Management Protocol) components: Manager, Agent, MIB, and compare SNMPv1/v2c (insecure) vs. SNMPv3 (authentication + encryption).
- Configure **Syslog** for centralized logging, identify severity levels (0–7), and explain the benefits of log aggregation and correlation using **SIEM** tools.
- Describe **NetFlow** for traffic analysis (who, what, when, where, how much) and distinguish it from **packet capture** (Wireshark) which captures full payloads.
- Explain **QoS** (Quality of Service) mechanisms including traffic classification (DSCP/CoS), queuing strategies (FIFO, priority, WFQ), and traffic shaping for voice/video prioritization.

8.1 Documentation: Maps for the Kingdom

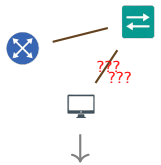
Why Document?

Without a map, the network is a murky swamp. If the Admin leaves, the knowledge leaves with them!

Two Types of Maps

1. **Physical Diagram**:
   - *Shows:* Racks, Cabling, Ports.
   - *Use:* "Where do I plug this cable?"
2. **Logical Diagram**:
   - *Shows:* IP Addresses, VLANs, Data Flow.
   - *Use:* "Why can't VLAN 10 ping VLAN 20?"

Undocumented Swamp



Documented Castle

Logical Map:
R1: 192.168.1.1
SW1: 192.168.1.2
PC1: 192.168.1.10
Physical Map:
Rack 2, U14
Port G0/1

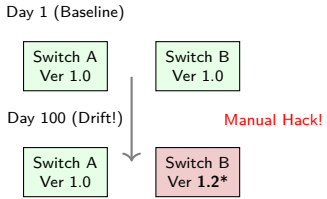
Configuration Management: Avoiding Chaos

The Concept

Managing device settings centrally to ensure consistency.

Key Terms

- **Baseline**: The "Golden Standard." How a device *should* be configured (Security rules, VLANs).
- **Drift**: When a device slowly changes from the baseline over time (e.g., someone makes a quick manual change and forgets to document it).



The Solution

Use automation tools (Ansible/Python) to force devices back to the Baseline!

Backups: Dragon Insurance

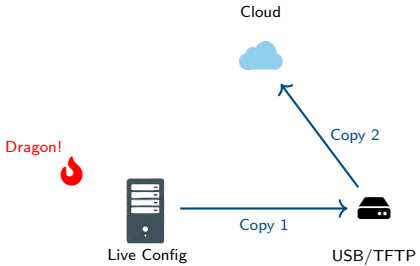
What to Backup?

It's not just files. You need:

1. **Configuration**: The 'running-config' text file.
2. **OS Image**: The IOS/Firmware file.
3. **State Data**: ARP tables, MAC tables (for forensics).

The 3-2-1 Rule

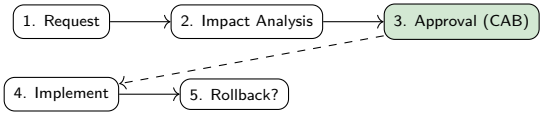
- **3** copies of data.
- On **2** different media types (Disk/Cloud).
- Keep **1** copy off-site (Far Far Away).



Change Management: The Royal Decree

Why we need Rules

Ogres are clumsy. If you smash a core switch without a plan, the kingdom goes dark. **Change Mgmt** minimizes risk.



Critical Component: Rollback

Before you change *anything*, you must answer: **"How do I undo this if it breaks the network?"**

Change Types

Standard: Routine (Reset Password).
Normal: Risky (New VLAN) -> Needs Approval.
Emergency: Fix it NOW! (Firewall down).

Case Study: Donkey's Unauthorized Wi-Fi

Scenario: "I'm making Waffles... and Wi-Fi!"

Donkey wants to stream music in the Swamp. He buys a cheap $20 Router from Best Buy and plugs it into the main Corporate Switch.

The Result:

- The Router broadcasts "Donkey-Guest" (Open/No Password).
- The Router starts handing out bad IP addresses (Rogue DHCP).
- Lord Farquaad's spies connect to it and access the internal Castle network.

Discussion

1. Which Change Management steps did Donkey skip?
2. What technical control could have stopped this immediately?

Case Study Solution

The Fix

- **Process Failure**: Donkey skipped **Request**, **Impact Analysis**, and **Approval**. This was an "Unauthorized Change." No Change Advisory Board (CAB) existed to say "Wait, what are you doing?"
- **Technical Fix**: Enable **Port Security** on the network switch. This feature limits how many MAC addresses (devices) can connect to a single port. When Donkey plugged in his router, it immediately tried to broadcast multiple MAC addresses (one for itself, plus virtual ones for DHCP). The port security rule would have violated the limit and **shutdown the port automatically**.
- **Alternative Control**: Implement **NAC (Network Access Control)**. This would scan Donkey's unauthorized router, see it is not on the approved device list, and either block it or quarantine it in a "guest" VLAN with restricted access.
- **Lesson**: Never skip the Change Management process, and always enforce technical controls like Port Security on access ports where regular users (and Donkeys) can plug things in.

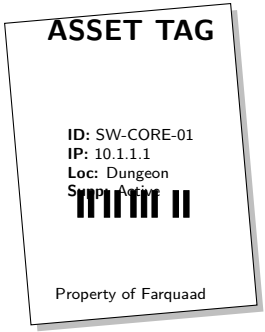
8.1 Asset Inventory: Counting the Swamp Creatures

The Problem

If you don't know what you own, you can't patch it, and you certainly can't secure it.

What to Track (The Tags)

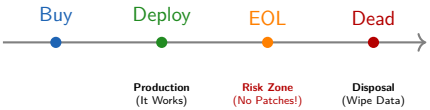
- **Hardware**: "Switch-01" (Serial #).
- **Location**: "Swamp Hut, Rack 2".
- **Owner**: "Donkey".
- **Lifecycle**: "Purchase Date" vs "Death Date".



Lifecycle Management: The Circle of Life

Hardware has a lifespan

Like onions (and ogres), hardware gets old and smelly.



The "EoL" Danger

End of Life (EoL) means the vendor stops making security patches. If you keep an EoL firewall, you are inviting the Dragon in.

Decommissioning

Wipe the disk! Don't sell a router on eBay with the Castle passwords still on it.

Physical Diagrams: The "Real World" Map

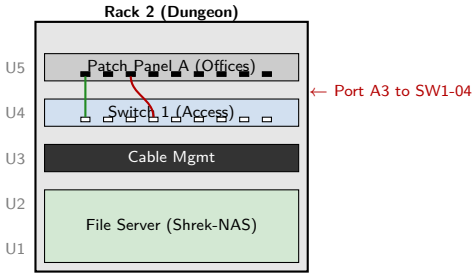
What it shows (Layer 1)

Used when you need to walk into the server room and touch something.

- **Location**: Building, Room, Rack Number.
- **Hardware**: Specific models, "U" positions.
- **Cabling**: Which patch port goes to which switch port?

Scenario

"Donkey, go to the Dungeon Server Room, Rack 2. Move the yellow cable from Switch 1, Port 5 to Port 6."



Logical Diagrams: The "Data Flow" Map

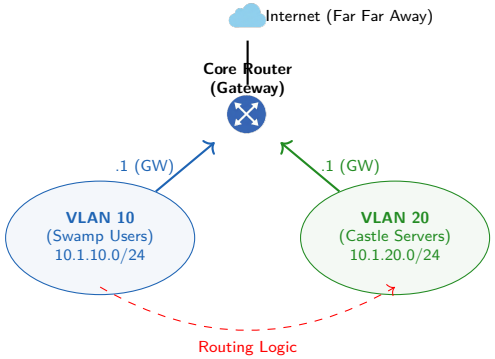
What it shows (Layer 3)

Used when you need to configure routing or firewalls.

- **Addressing**: IP Subnets / CIDR.
- **Grouping**: VLANs, Trust Zones.
- **Routing**: Gateways, WAN links.

Comparison

Physical: "The cable is plugged into Port 2."
Logical: "The traffic flows from the User Subnet to the Server Subnet."



IPAM: The Royal Guest List

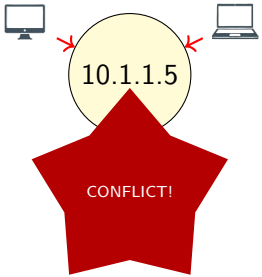
IP Address Management (IPAM)

You cannot have two Ogres sitting in the same chair.

- **Conflict**: Two devices with IP 10.1.1.5 = Network Crash.
- **Exhaustion**: Running out of IPs in the DHCP pool.

Tools

Don't use an Excel spreadsheet! Use **NetBox** or **phpIPAM**.



Agreements: The Royal Treaties

Definitions

When Shrek hires Puss in Boots, they sign a contract.

SLA

Service Level Agreement
The Promise.
"I will catch 99.9% of mice."
(Binding Contract)

NDA

Non-Disclosure Agreement
The Secret.
"You cannot tell anyone where the Swamp is."
(Legal Privacy)

MOU

Memo of Understanding
The Handshake.
"We agree to work together on this quest."
(Less Formal)

8.2 Host Discovery: "Who Goes There?"

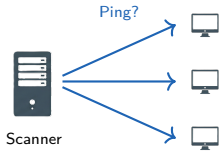
The Goal: Visibility

Shrek cannot defend the Swamp if he doesn't know who is in it.

- Finding Rogue Devices (Spies).
- Checking Open Ports (Unlocked Doors).

Tools

Ping Sweeps: Yelling "Is anyone there?" **ARP Scans**: Asking "Who has this IP?"



Discovery: Shouting vs. Listening

Active Discovery (Shouting)

Sending packets to devices to provoke a response.

- *Ex:* Nmap, Ping.
- **Pro:** Fast, accurate.
- **Con:** Noisy, might crash fragile IoT devices.

Passive Discovery (Listening)

Just listening to network traffic (like sniffing the air).

- *Ex:* Wireshark, NetFlow.
- **Pro:** Stealthy, zero impact.
- **Con:** Takes longer, misses silent devices.

Active (Loud)

Passive (Quiet)

Nmap Concepts: The Three States of a Door

What is Nmap asking?

When Nmap scans an IP, it knocks on every "Door" (Port) and categorizes the response into three main states.

1. OPEN (Success)

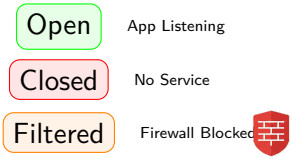
Response: "Come in!" (SYN-ACK).
Meaning: An application is listening. *Risk: This is an entry point for hackers.*

2. CLOSED (Rejection)

Response: "Go away!" (RST).
Meaning: The device is up, but nothing is running on that port.

3. FILTERED (The Void)

Response: Silence... (Timeout).
Meaning: A Firewall (Dragon) blocked the packet. Nmap doesn't know if the port is open or closed.



Nmap in Action: Reading the Output

Terminal - Nmap Scan

```
root@swamp:~# nmap -A 10.1.1.5
Starting Nmap 7.94...
Nmap scan report for donkey-pc (10.1.1.5)
Host is up (0.002s latency).

PORT STATE SERVICE VERSION
22/tcp open ssh OpenSSH 8.2p1
80/tcp open http Apache httpd 2.4.41
443/tcp closed https

OS details:  Linux 4.15 - 5.6
Service Info:  OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Decoding the Scan

- **-A**: Aggressive! (Gets OS and Versions).
- **PORT**: The number (e.g., 80 is Web).
- **STATE**: Open/Closed.
- **VERSION**: Crucial for hackers! "Apache 2.4.41" might have a specific bug we can exploit.
- **OS**: Nmap guesses this is a Linux machine (likely Ubuntu) based on how it talks.

Scan Techniques: Stealth vs. Noise

TCP Connect (-sT)

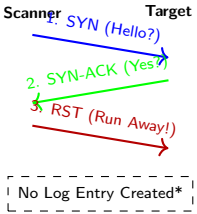
The "Polite" Knock.

- Complete 3-Way Handshake.
- **Con:** Shows up in system logs immediately. Shrek will hear you.

SYN Scan (-sS)

The "Ding-Dong-Ditch".

- Send SYN, get response, then send RST (Reset).
- Never establishes a full connection.
- **Pro:** Faster and stealthier.



Timing Flags (-T)

-**T0** (Paranoid) to -**T5** (Insane).

- -**T4** is standard/fast.
- -**T1** is super slow (sneaky).

Case Study: Puss in Boots' Reconnaissance

Scenario

Puss has been hired to test the Swamp's security. Shrek says: "Find out what ports are open, but **don't wake up the babies** (don't crash anything)."

Target: 10.0.0.0/24 subnet. **Constraints:** Business hours (9am-5pm).

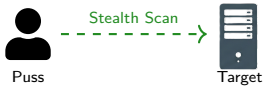
Strategy Questions

1. Should Puss use a loud "Connect" scan or a stealthy "SYN" scan?
2. Should he scan all 65,535 ports or just the Top 100?
3. How can he identify if the server is running Windows?

Case Study Solution

Puss's Plan

1. **Discovery:** Use 'nmap -sn' first just to see what is alive (Ping Sweep). Low impact.
2. **Port Scan:** Use 'nmap -sS' (SYN Scan) because it is stealthier and lighter on network traffic.
3. **Depth:** Scan top 100 ports first. Full scans happen after hours.
4. **OS Detect:** Use 'nmap -O' carefully (it sends weird packets to confuse the target).



Discovery Protocols: "Hello Neighbor!"

The Concept

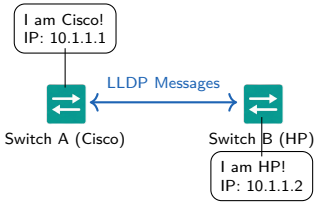
Network devices act like friendly neighbors. Every 60 seconds, they shout their details to anyone connected to them.

What they shout (The Risk)

- "My Name is **Core-Router-01**."
- "My Management IP is **10.1.1.1**."
- "I am running **Cisco IOS v15.2**."
- "You are plugged into **Port Gi0/1**, **VLAN 10**."

The Protocols

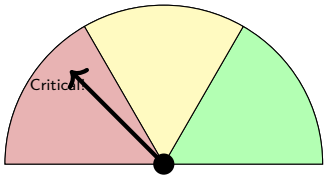
- **CDP (Cisco Discovery Protocol)**: Proprietary. Only works between Cisco devices.
- **LLDP (Link Layer Discovery Protocol)**: Industry Standard (IEEE 802.1AB). Works on everything.



Performance Monitoring: Checking the Pulse

Key Metrics (The Vital Signs)

- **Bandwidth**: "Is the pipe full?" (Utilization %).
- **Latency**: "Ping time." How long for data to travel?
- **Jitter**: "Lag Spikes." Variation in latency. (Killer for VoIP and Gaming).
- **Packet Loss**: "Dropped Letters." Data destroyed in transit (Bad cables or congestion).



Link Saturation

Baselines

You need to know what "Normal" looks like. *Is 80% CPU usage bad? Not if it's always at 80% doing video rendering.*

Availability: Is the Drawbridge Down?

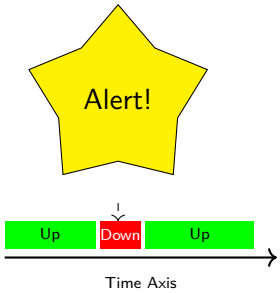
Availability = Uptime

"Can users actually do their work?"

Ping vs. Service Check

- **Ping (ICMP)**: "Is the server on?" (Lights are on).
- **Service Check (TCP)**: "Is the Web Server running?" (The store is open).

A server can respond to Ping but still show a "404 Error" website!



The "Five Nines"

99.999% Uptime means only 5 minutes of downtime per year. This is the gold standard for Enterprise Networks.

Configuration Monitoring: Who Changed the Settings?

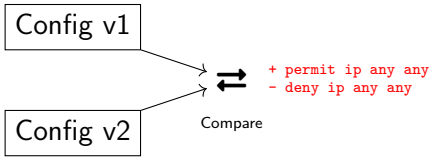
Configuration Drift

The network rots over time because people make quick, manual changes and forget to undo them.

- "I'll just open the firewall for testing."
- *3 months later* → Firewall is still open.

The Solution (RANCID)

Tools that automatically backup configs every night and compare them. If a line changed, Shrek gets an email!



8.3 SNMP: The Royal Messengers

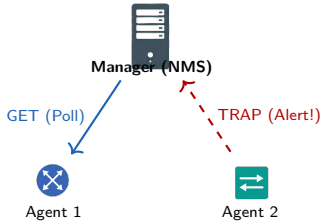
Simple Network Management Protocol

How we talk to devices without logging into them.

- **Manager (NMS)**: The King (Server) who asks questions.
- **Agent**: The Peasant (Router) who answers.

The "Restaurant" Analogy

- **MIB**: The Menu (List of all possible questions).
- **OID**: The Item Number (e.g., .1.3.6... = "CPU Temp").



Ports

UDP 161 (Polling) / **UDP 162** (Traps)

SNMP Operations: Asking vs. Yelling

1. Polling (GET)

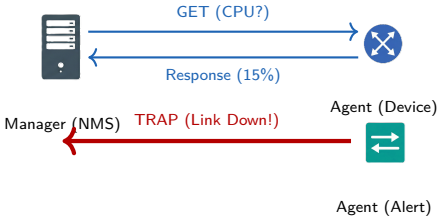
The Manager asks the Agent a question.

- **GET**: Read a value (e.g., "What is your uptime?").
- **SET**: Change a setting (e.g., "Turn off Port 1").
- **Walk**: Ask for the entire inventory.

2. Traps (Alerts)

The Agent yells at the Manager because something broke.

- Sent immediately without being asked.
- Examples: "Fan Failure", "Link Down", "Overheating".



SNMP Versions: Evolution of Security

Version History

1. **SNMPv1**: The original. No security.
2. **SNMPv2c**: Faster (Bulk transfers), but still **Cleartext**.
3. **SNMPv3**: **Secure**. Adds Encryption + Authentication.

The Community String Risk

In v1/v2c, the "Password" is called a Community String.

- Defaults: **public** (Read Only) / **private** (Read/Write).
- Sent in **Cleartext**! Anyone with Wireshark can steal it and map your network.

Ver	Security	Notes
v1	None	Original; cleartext
v2c	None	Faster (bulk); cleartext
v3	Auth + Enc	Users, AES/3DES, hashes

Case Study: Lord Farquaad's Open Door

Scenario: "Welcome to Duloc"

Lord Farquaad set up SNMP monitoring on all his castle switches. Because he was in a rush, he used the default settings:

- **Version**: SNMPv2c.
- **Community String**: "public".

Robin Hood sat in the bushes with a laptop and ran a tool called 'snmpwalk'. Within seconds, he downloaded the entire network map, including IP addresses, router models, and uptime stats.

Discussion Questions

1. What specific vulnerability allowed Robin Hood to read the data?
2. Did Robin Hood need a complex password cracker to do this?
3. What is the industry-standard way to fix this vulnerability?

Case Study Solution: Lord Farquaad's Open Door

The Answers

1. **Vulnerability**: **Cleartext Community Strings**. "public" is the default string known by every hacker on earth.
2. **No Cracker Needed**: It was an "Open Door." He just asked the routers nicely using the default password.
3. **The Fix**: Upgrade to **SNMPv3**. It uses **AuthPriv** (Authentication + Privacy/Encryption), so even if Robin Hood captures the packets, he can't read them.

8.4 Syslog: The Royal Scribe

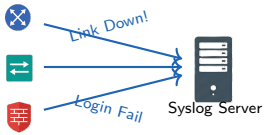
The Standard Diary

Network devices don't have screens. They need a place to write down what is happening.

- **Syslog (Protocol)**: UDP 514.
- **Centralized Logging**: Devices send logs to a single server (The Scribe) so you don't have to log into 50 switches to check for errors.

The Components

Facility: "Who is speaking?" (Kernel, Mail, User).
Severity: "How bad is it?" (0 to 7).



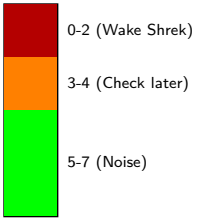
Syslog Severity Levels: 0 to 7

The Scale (Lower = Worse)

#	Name	Meaning
0	**Emergency**	System is dead (Panic).
1	**Alert**	Action needed NOW.
2	**Critical**	Critical error (RAM fail).
3	**Error**	Standard error message.
4	**Warning**	Event occurred (Link flap).
5	**Notice**	Normal but significant.
6	**Info**	Just information.
7	**Debug**	EVERYTHING (Developer).

Mnemonic

Every **A**lert **C**reates **E**rrors **W**hen **N**etworks **I**nterrupt **D**onkey.



SIEM: The Magic Mirror

Security Information & Event Mgmt

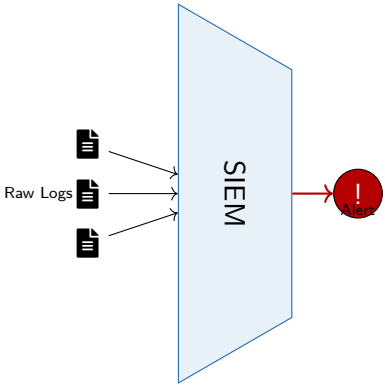
Syslog collects logs. **SIEM** understands them.

- **Aggregation**: Collects logs from Everywhere (Server, Firewall, Door Badge).
- **Correlation**: Connects the dots.
- **Alerting**: Tells the Admin.

Correlation Example

1. Badge Reader: "Puss entered building at 2AM."
2. Server: "Puss logged into Database."
3. Firewall: "Database sending 5GB to Internet."

SIEM Conclusion: **Data Theft!**



Case Study: The Silent Failure

Scenario: "Why is the bridge up?"

The Castle Drawbridge (Router) stopped working at 3:00 AM. Traffic stopped flowing.
Shrek wakes up at 8:00 AM. He logs into the Router, but the logs only go back to 7:00 AM because the buffer overwrote the old messages. He has no idea why it crashed.

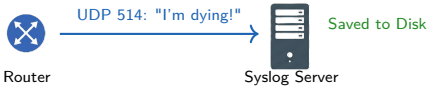
Discussion Questions

1. Where were the logs stored (Locally vs. Remotely)?
2. Why did the logs disappear?
3. What tool would have saved the 3:00 AM error message?

Case Study Solution: The Silent Failure

The Fix

1. **Storage**: They were stored in **RAM** (Buffered Logging). When RAM fills up, old logs are deleted.
2. **Reason**: Lack of persistence. Also, if the router rebooted, RAM logs would be lost entirely.
3. **Tool**: A **Syslog Server**. The router should have sent the critical error ("Fan Failure") to the server immediately at 3:00 AM. Shrek could read it later.



8.5 Traffic Analysis: NetFlow vs. Packet Capture

1. NetFlow (Metadata)

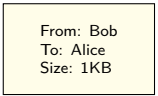
The Phone Bill.

- Shows *who* called *whom*, *when*, and for *how long*.
- Does **NOT** show what they said.
- *Use:* Bandwidth hogs, DDoS detection.
- **Lightweight**.

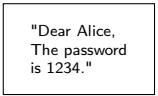
2. Packet Capture (PCAP)

The Wiretap.

- Records the actual **content** of the conversation.
- Shows the passwords, emails, images.
- *Use:* Deep troubleshooting, Forensics.
- **Heavy** (Needs huge storage).



NetFlow (Envelope)



PCAP (Content)

NetFlow / IPFIX: Watching the River

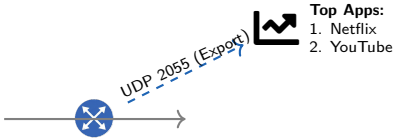
How it works

Routers summarize traffic into "Flows" and send the summary to a Collector.

- Source IP / Dest IP.
- Source Port / Dest Port.
- Protocol (TCP/UDP).
- Byte Count.

Finding the "Top Talker"

"Why is the internet slow?" **NetFlow says:** "Because Donkey's iPad (10.1.1.50) is downloading 4TB of movies from Netflix."



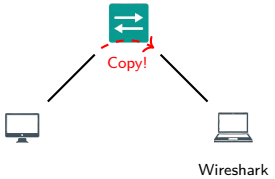
Packet Capture: The Microscope

Tools

- **Wireshark**: The GUI analyzer.
- **tcpdump**: Command line capture (Linux).

Port Mirroring (SPAN)

Switches normally keep secrets. To capture traffic not meant for you, you must configure a **SPAN Port** (Switched Port Analyzer). *"Copy all traffic from Port 1 to Port 2 (My Sniffer)."*



tcpdump: The Command Line Sniffer

Terminal - tcpdump

```
root@swamp: # tcpdump -i eth0 -n port 80

tcpdump: verbose output suppressed...
listening on eth0, link-type EN10MB...
10:42:01.52 IP 10.1.1.5.54321 > 10.1.1.1.80: Flags
[S]...
10:42:01.53 IP 10.1.1.1.80 > 10.1.1.5.54321: Flags
[S.]...
10:42:01.54 IP 10.1.1.5.54321 > 10.1.1.1.80: Flags
[.]...
3 packets captured
```

Decoding the Output

- **Source**: 10.1.1.5 (Port 54321)
- **Dest**: 10.1.1.1 (Port 80 / Web)
- **Flags [S]**: SYN packet (Start of connection)

Why use tcpdump?

- **No GUI**: Servers usually don't have screens. You can't use Wireshark on a headless router.
- **Speed**: Great for quick checks ("Is traffic hitting this interface?").

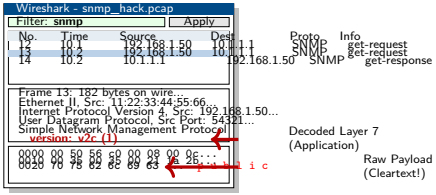
Key Flags

- **-i eth0**: Listen on interface eth0.
- **-n**: No DNS (Show IPs, don't wait to resolve names).
- **-w capture.pcap**: Save to a file (Write).
- **port 80**: Only show web traffic.

Pro Tip

Capture with `tcpdump -w file.pcap` on the server, then download the file and open it in Wireshark for ease of use!

Wireshark: Anatomy of a Packet Capture



2. Details (Layers)

"The Inspection." Breaks down the packet by OSI Layer.

- Frame (L1)
- Eth (L2)
- IP (L3)
- UDP (L4)
- SNMP (L7)

3. Bytes (Hex)

"The Raw Data." What actually went over the wire.

8.6 Quality of Service (QoS): The VIP Lane

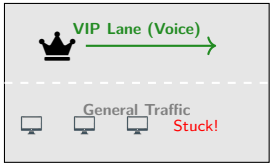
The Problem

Bandwidth is limited. If Donkey downloads a 4K movie while Shrek is on a Video Call, the video will freeze.

The Solution: QoS

Prioritization. Giving critical traffic (Voice/Video) a "Fast Pass" to skip the line.

- **High Priority**: Voice (VoIP), Video.
- **Low Priority**: Email, YouTube, Donkey's downloads.

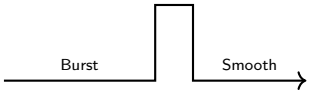


Managing Bandwidth: Shaping vs. Policing

Traffic Shaping (The Buffer)

"Please Wait."

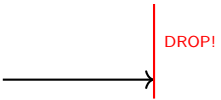
- Delays excess packets in a queue (Buffer).
- Smooths out bursts.
- *Analogy:* A waiting room.



Traffic Policing (The Chop)

"Get Out!"

- Drops excess packets immediately.
- Hard limit.
- *Analogy:* A bouncer cutting the line.



Classification: Stamping the Envelope

How does the router know?

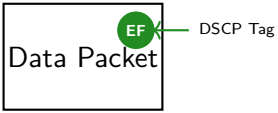
We add a "Tag" to the packet header so routers know it is VIP.

Layer 2: CoS (Class of Service)

- Lives in the **802.1Q VLAN Header**.
- Range: 0 (Best Effort) to 7 (Network Control).
- **Voice usually = 5**.

Layer 3: DSCP (DiffServ Code Point)

- Lives in the **IP Header**.
- **EF (Expedited Forwarding)**: The absolute highest priority for Voice.



Case Study: The Robot Voice

Scenario: "I c-c-can't h-hear y-you!"

Shrek is trying to call Fiona using VoIP (Voice over IP). The audio sounds robotic and choppy. Meanwhile, the 3 Blind Mice are streaming 4K movies in the next room.

Diagnosis:

- **Bandwidth**: Saturated by movies.
- **Jitter**: Voice packets are arriving late and out of order.

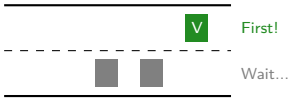
Discussion Questions

1. Which metric is ruining the call: Latency or Jitter?
2. How can we fix this without banning movies entirely?
3. What DSCP tag should the VoIP phones be using?

Case Study Solution: The Robot Voice

The Fix: Apply QoS

1. **Root Cause**: **Jitter**. (Variation in arrival time makes voice sound robotic).
2. **Strategy**: Configure **Queuing** on the router.
   - Create a "Low Latency Queue" (LLQ) for Voice.
   - Put the Movies in the "Best Effort" queue.
3. **Tagging**: Ensure VoIP phones mark traffic as **EF (Expedited Forwarding)** or **DSCP 46**.



Module 8.0 Summary I

Key Concepts:

- **Physical diagrams**: Show racks, cables, port connections. **Logical diagrams**: Show IP addresses, VLANs, subnets, routing.
- **Configuration management**: Use standardized naming, regular backups, version control, and change control boards (CCB) for controlled modifications.
- **Network lifecycle**: Procurement $\rightarrow$ Deployment $\rightarrow$ Maintenance $\rightarrow$ End-of-Life (EoL) planning $\rightarrow$ Secure disposal.
- **Baselines**: Establish normal performance metrics (bandwidth, latency, CPU) to identify anomalies and security incidents.
- **IPAM**: Centralized IP address management. Track assignments, detect conflicts, integrate with DHCP/DNS. Prevent IP exhaustion.
- **CDP** (Cisco proprietary): Neighbor discovery every 60 sec. **LLDP** (IEEE 802.1AB): Vendor-neutral standard. Both map Layer 2 topology.

Module 8.0 Summary II

- **SNMP**: Manager polls Agents using **MIB** (Management Information Base). SNMPv3 adds authentication (authNoPriv) and encryption (authPriv). Traps = unsolicited alerts.
- **Syslog**: Centralized logging. Severity 0 (Emergency) to 7 (Debug). Use **SIEM** (Security Information and Event Management) for correlation and alerting.
- **NetFlow**: Collects traffic metadata (source/dest IP, ports, protocol, bytes, packets). Flows exported to Collector for analysis (NetFlow Analyzer).
- **Packet capture**: Wireshark captures full frame contents for deep inspection. Privacy/legal concerns. Use for troubleshooting, not routine monitoring.

Module 8.0 Summary III

Quality of Service (QoS):

- **Classification**: Mark traffic using **DSCP** (Layer 3, 0–63) or **CoS** (Layer 2, 0–7). Voice = DSCP 46 (EF), Video = DSCP 34 (AF41).
- **Queuing**: FIFO (first-in-first-out), Priority Queue (low-latency for voice), WFQ (weighted fair queuing for balanced sharing).
- **Traffic shaping**: Smooth bursty traffic to match bandwidth limits. **Policing**: Drop excess traffic exceeding rate.
- Use QoS to prioritize latency-sensitive traffic (VoIP, video conferencing) over bulk data (file transfers, backups).