- **1. Traffic Volume & Patterns**
  - **Bandwidth over time** (already done)
    - **Bandwidth is a foundational metric in network characterization because it reveals the volume of data traversing a network over time, offering insight into both expected usage patterns and anomalies.** By monitoring bandwidth, analysts can detect events such as large file transfers, data exfiltration, denial-of-service (DoS) attacks, or unusually quiet periods that may suggest stealthy behavior. Consistent bandwidth trends can help establish baselines for normal operations, while sudden spikes or drops may indicate operational changes, misconfigurations, or malicious activity. Additionally, comparing bandwidth across VLANs, protocols, or specific hosts enables more granular understanding of where and how network resources are being consumed, making it an essential metric for performance tuning, threat detection, and capacity planning.
  - **Packet rate over time** (done)
    - **Measuring how many packets are transmitted over time is a key metric for understanding the pace and behavior of network communication.** Unlike bandwidth, which reflects data volume, packet rate reveals how frequently devices are talking, regardless of payload size. High packet rates can indicate scanning activity, control signaling, or chatty protocols like VoIP or DNS. Sudden surges may point to denial-of-service attempts or malware beaconing, while unusually low rates might suggest outages or suppressed communications. When analyzed across time and segmented by source, destination, or VLAN, packet rate helps distinguish between bulk data transfers and lightweight control traffic, offering valuable insight into the operational rhythm and health of a network.
  - **Average packet size** (done)
    - **Packet size (or more accurately, frame size) provides critical insight into the nature of network traffic, helping differentiate between control signals, typical user behavior, and potentially malicious activity.** Small packets are often associated with frequent, lightweight communication—like keep-alives, beacons, or scanning—while large packets usually indicate file transfers, video streams, or data exfiltration. Monitoring average packet size over time can help identify shifts in application behavior, such as the start of a large upload or the presence of tunneling techniques that pad or split

traffic. Sudden deviations from the normal size profile may signal changes in protocol usage, covert channels, or emerging performance issues. In network characterization, packet size complements bandwidth and packet rate to form a more complete picture of what the traffic is doing—not just how much or how fast.

- **Burst detection** — sudden spikes in traffic volume (done)
    - **Burst detection identifies short, intense spikes in network activity that deviate from normal traffic patterns, making it a powerful tool for uncovering unusual or potentially malicious behavior.** These bursts might represent large file transfers, sudden scanning activity, or command-and-control (C2) communications that occur in quick, periodic intervals to evade detection. Because many attacks or unauthorized data movements happen in brief windows to avoid triggering volume-based alarms, detecting bursts helps analysts focus on high-impact moments that might otherwise be buried in overall traffic. Burst detection also highlights transient issues like micro-outages or sudden load surges from legitimate applications, offering value not just for security, but also for performance monitoring and capacity planning. It adds temporal precision to network characterization by revealing when abnormal traffic is happening, not just that it is.
- **Traffic by VLAN** or subnet — who's talking most (done)
    - **Analyzing traffic by VLAN (Virtual Local Area Network) allows for segmentation-aware network characterization, offering a clearer understanding of how different parts of the network behave and interact.** VLANs are often used to logically separate users, devices, or functions—such as isolating administrative traffic from user traffic or separating departments. By monitoring bandwidth, packet rate, and protocol usage on a per-VLAN basis, analysts can detect anomalies specific to each segment, such as unexpected communication between VLANs, misuse of privileged network zones, or uneven load distribution. It also helps pinpoint performance issues or security threats within specific network boundaries, making troubleshooting and response more targeted and effective. VLAN-level visibility adds necessary context to raw traffic data, aligning technical observations with the intended network architecture.

🔹 **2. Flow & Host Analysis**

- **Top talkers** by bytes/packets sent (done)
    - **Top talkers—hosts that generate the most traffic—are essential to network characterization because they reveal which devices are most active and potentially most influential in the network's behavior.** Monitoring top talkers helps identify normal usage patterns, such as servers handling large volumes of client requests, as well as abnormal ones, like a workstation suddenly initiating outbound connections to many external IPs. Shifts in top talker rankings between baseline and event periods can signal data exfiltration, lateral movement, malware communication, or unauthorized application use. By focusing attention on high-traffic nodes, analysts can quickly narrow investigations, assess the potential impact of incidents, and verify whether critical assets are behaving as expected.
- **Top listeners** — heavy receivers (done)
    - **Top listeners—hosts that receive the most network traffic—provide crucial visibility into which systems are being targeted, accessed, or relied upon within a network.** These devices may include servers providing legitimate services, but they can also be endpoints under attack, recipients of lateral movement attempts, or command-and-control nodes awaiting instructions. Monitoring top listeners helps distinguish between expected behavior (e.g., a web server receiving steady inbound requests) and suspicious activity (e.g., a user device suddenly receiving large volumes of internal traffic). Changes in listener roles between baseline and event traffic can reveal pivot points, unauthorized services, or data collection hubs. As a counterpart to top talkers, identifying top listeners enriches situational awareness and supports a more complete understanding of network dynamics.
- **New or rare conversations** — identify previously unseen IP pairs (done)
    - **New or rare connections are powerful indicators of behavioral change within a network and are often the first sign of compromise, lateral movement, or data exfiltration.** By comparing current traffic against a known-good baseline, analysts can flag communications between hosts that have never—or only infrequently—interacted. These anomalies may represent malware propagation, unauthorized access attempts, or internal reconnaissance as an attacker maps the network. Even in benign scenarios, rare connections can uncover misconfigured devices, newly deployed

services, or shadow IT. Tracking and analyzing new or rare connections provides an early warning system for emerging threats and helps ensure that traffic aligns with intended network design and access controls.

- **Flow duration analysis** — how long conversations last
- **Flow fanout** — # of unique destinations per source (good for spotting scanners or beacons)

🔹 **3. Anomaly Detection**

- **Unusual protocols/ports** (you're doing this)
    - **Unusual ports or protocols can be strong indicators of unauthorized activity, making them a critical component of network characterization and threat detection.** Most environments operate with a predictable set of ports and protocols—such as HTTP, HTTPS, DNS, and SMB—so deviations from this baseline can signal scanning activity, command-and-control (C2) traffic, or the use of custom or covert communication channels. Attackers often exploit uncommon ports or tunnel protocols through allowed ones to bypass firewalls and monitoring systems. By identifying spikes in usage of rarely seen ports or unexpected protocol shifts, analysts can uncover stealthy behaviors, misconfigurations, or policy violations. Monitoring this metric enhances situational awareness and helps ensure the network is being used as intended.
- **Z-score or IQR outliers** in:
    - Port/protocol use
    - Byte/packet volume per host

🔹 **4. Jitter, Latency, Timing**

- **Jitter per flow** or VLAN (done)
    - **Jitter— the variation in time between successive packets—offers valuable insight into the stability and consistency of network communication, making it a useful metric for both performance monitoring and anomaly detection.** In real-time applications like VoIP,

video conferencing, or industrial control systems, high jitter can cause noticeable degradation, such as choppy audio or delayed commands. From a security perspective, abnormal jitter may indicate covert channels, traffic shaping, or the presence of obfuscation techniques like timing-based command-and-control (C2). By analyzing jitter patterns over time and across VLANs or host groups, analysts can detect performance issues or behavioral shifts that aren't evident in bandwidth or packet count alone. This makes jitter a key complement to volume-based metrics in understanding how traffic is flowing—not just how much of it there is.

🔹 **5. Protocol & Port Usage**

- **Application fingerprinting** by port (e.g., is someone running HTTP on a weird port?)
    - **Application fingerprinting involves identifying the specific applications or services generating network traffic, and it plays a critical role in network characterization by revealing what is communicating—not just how much or how often.** Each application has unique patterns in terms of port usage, packet sizes, timing intervals, and protocol behaviors. By fingerprinting these traits, analysts can differentiate between legitimate traffic (like web browsing, email, or cloud services) and suspicious or unauthorized activity (such as tunneling, P2P apps, or malware communication). This visibility helps enforce policy, detect rogue applications, and understand the functional use of network resources. Fingerprinting also supports threat hunting by matching traffic signatures to known malicious tools, enabling faster detection and response.
- **Protocol entropy** — # of distinct protocols over time
    - **Protocol entropy measures the diversity and distribution of protocols used in network traffic, offering a quantitative view of how communication patterns evolve over time.** High entropy indicates a wide variety of protocols in use, which may be normal in dynamic environments but could also suggest complex or chaotic traffic during an incident. Low entropy, on the other hand, may reflect centralized command-and-control activity, the suppression of normal communication, or the use of a single protocol for tunneling or exfiltration. By tracking changes in protocol entropy, analysts can detect shifts in network behavior that aren't visible through volume-based metrics alone. This makes it a valuable tool for identifying

abnormal usage patterns, classifying network segments, and supporting both threat detection and operational diagnostics.

- **Unexpected combinations** (e.g., UDP on port 80)
    - **Unexpected combinations—such as unusual pairings of IP addresses, ports, VLANs, or protocols—can signal deviations from normal network behavior and are often early indicators of compromise or misconfiguration.** In well-understood environments, certain hosts are expected to communicate only with specific services using known protocols and ports. When those relationships change—like a user workstation initiating connections to a database server on an unapproved port or two isolated VLANs suddenly exchanging traffic—it may point to lateral movement, policy violations, or malicious activity. Tracking and flagging these unexpected combinations helps uncover stealthy or unauthorized behavior that might otherwise go unnoticed, reinforcing both security monitoring and architectural compliance.

🔹 **6. Security Indicators**

- **Port scans** — many unique ports from one source
    - **Port scans are a common reconnaissance technique used to discover open services on a host, and detecting them is essential for understanding potential threats and mapping early-stage attack activity within a network.** While not inherently malicious, port scans often precede exploitation attempts by revealing which systems are listening on which ports. By monitoring for scan-like behavior—such as a single host sending packets to many ports on one or more destinations—analysts can identify compromised devices conducting internal reconnaissance, external attackers probing for vulnerabilities, or even misconfigured tools. Recognizing port scans helps differentiate benign traffic from probing activity and allows defenders to respond before an actual breach occurs. It also informs access control and segmentation policies by highlighting which services are exposed and potentially at risk.
- **Lateral movement** — same source hitting multiple internal Ips
    - **Lateral movement refers to the technique attackers use to navigate through a network after gaining an initial foothold, and detecting it is**

crucial for identifying active compromises and limiting their spread. This phase often involves a compromised host attempting to access new internal systems, using legitimate credentials or exploiting vulnerabilities to elevate privileges and expand control. By characterizing lateral movement—such as new or rare internal connections, high fan-out behavior, or repeated access to common ports across multiple hosts—analysts can detect attackers in motion, even if the initial intrusion went unnoticed. Recognizing lateral movement helps distinguish targeted attacks from normal user behavior, supports incident response by identifying affected assets, and strengthens network segmentation strategies to contain future breaches.

- **Fan out analysis**
    - **Fan-out analysis examines how many distinct destinations a single host communicates with, providing a valuable lens for detecting scanning, reconnaissance, or lateral movement within a network.** In typical operations, most devices interact with a relatively small, consistent set of peers—like a workstation accessing a file server or a printer. A sudden increase in the number of unique connections from one host, especially over a short time frame, may indicate malicious behavior such as a port scan, worm propagation, or an attacker attempting to pivot through the network. Fan-out patterns are especially useful for identifying stealthy intrusions where traffic volumes remain low but connection diversity is high. By highlighting abnormal outreach behavior, fan-out analysis helps surface compromised systems, unauthorized access attempts, or misconfigured devices, making it a powerful tool in proactive threat detection and network hygiene monitoring.
- **Port-target mapping**
    - **Port-target mapping tracks which destination ports are accessed across different target hosts, helping to uncover patterns of reuse that may indicate coordinated or malicious behavior.** In a typical enterprise environment, services like SSH, HTTP, or SMB are accessed on a limited set of systems. When a single source host begins connecting to the same port (e.g., 445 or 3389) across many different

destinations, it can suggest lateral movement, service discovery, or exploitation attempts. This pattern is common during internal reconnaissance or when malware is programmed to seek out specific vulnerabilities. By visualizing how ports are being used across hosts, port-target mapping reveals both intended service access and potential abuse, supporting faster detection of attack propagation and reinforcing segmentation and access control strategies.

    - **New peer detection**
        - **Near-peer detection focuses on identifying new or unusual communications between devices that operate within the same role, subnet, or organizational function—often a subtle indicator of lateral movement or internal compromise.** In a well-segmented network, peers such as workstations in the same department typically have little reason to communicate directly with one another. When those connections begin to appear—especially if they weren't present in the baseline—it may indicate that a compromised host is probing or spreading to nearby systems. Detecting these near-peer interactions helps uncover low-noise, high-impact attack behavior that evades traditional volume-based metrics. It also supports policy enforcement, ensuring that access boundaries between devices of similar type or role are maintained as intended.

- **Command and Control patterns** — small, regular flows to remote IPs
- **Beaconing detection** — periodic low-volume connections