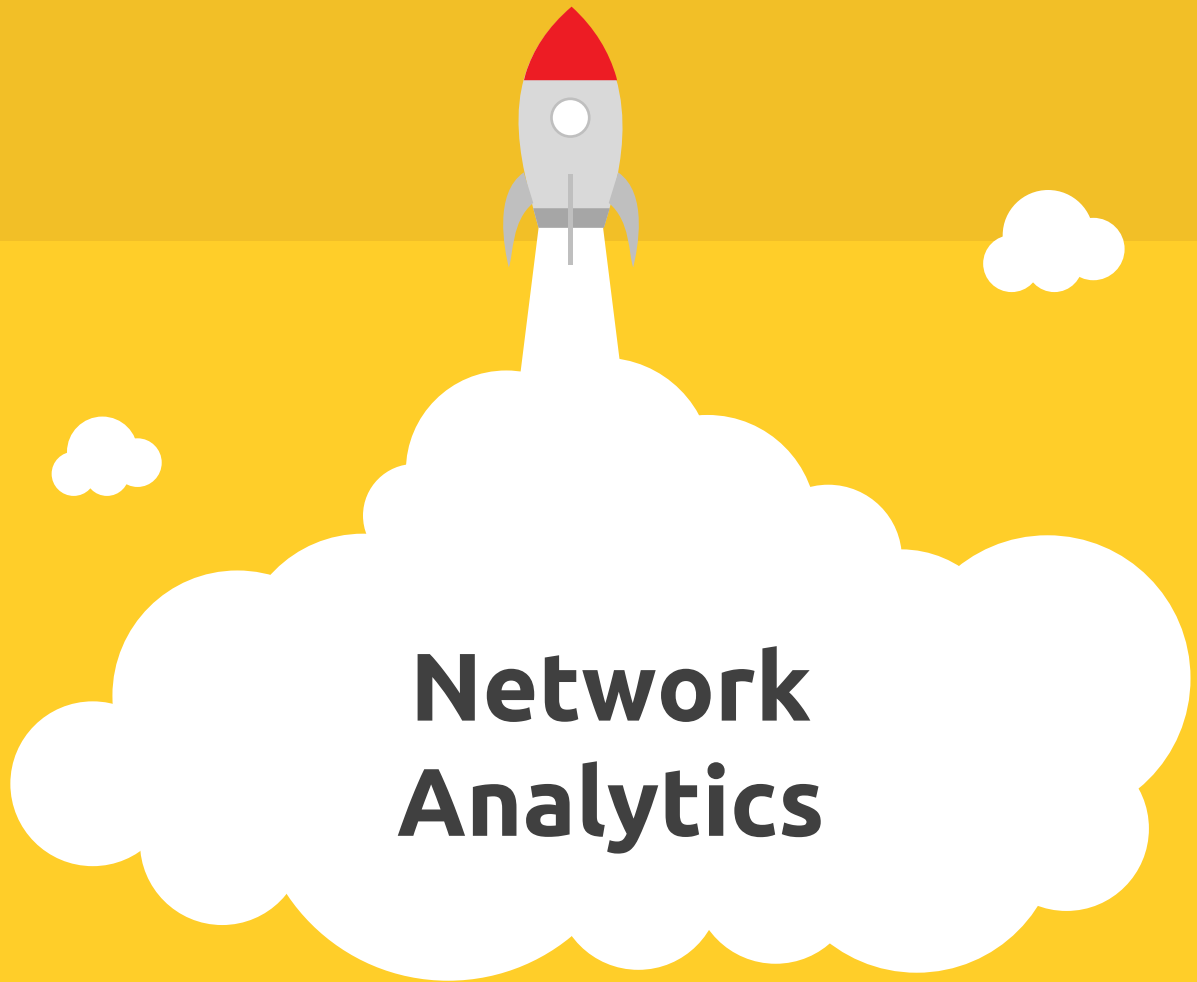
NT706050

NETWORK ANALYTICS WITH MACHINE LEARNING & DATA SCIENCE

Eng. Isuru Shanaka Lakmal
Mphil.(Reading), PG.Dip.(IA), B.Sc.(Hons.) Eng, M(IEEE), AM(IESL), AEng(ECSL)


Network
Analytics

Network Analytics

- Network analytics is the practice of analyzing network data to gain insights into the **performance**, **security**, and **behavior** of computer networks.
- It involves the **collection**, **processing**, and **analysis** of network data using various techniques and tools to **identify patterns**, **detect anomalies**, and **optimize network performance**.
- The ultimate goal of network analytics is to enable network operators and administrators to make data-driven decisions that improve the **reliability**, **security**, and **efficiency** of computer networks.

Network Analytics

The main requirements of network analytics

1. **Real-time monitoring**: Network analytics tools should be able to monitor network traffic in real-time to detect anomalies and performance issues.

2. **Data collection**: Network analytics tools should be able to collect and store data from various sources, including network devices, applications, and servers.

3. **Data processing**: Network analytics tools should be able to process large amounts of data quickly and efficiently to identify patterns, trends, and anomalies.

Network Analytics

The main requirements of network analytics

4. **Visualization:** Network analytics tools should be able to visualize data in an intuitive and easy-to-understand manner, using graphs, charts, and other visual aids.

5. **Security**: Network analytics tools should be able to detect and respond to security threats, including malware, phishing attacks, and other types of cyberattacks.

6. **Integration**: Network analytics tools should be able to integrate with other IT systems, such as security information and event management (SIEM) systems, to provide a comprehensive view of network activity.

Network Analytics

Network analytics tools

- **Wireshark**: A popular and widely-used network protocol analyzer that allows you to see what's happening on your network at a microscopic level. It's available for Windows, Mac, and Linux and is free to use.

- **PRTG Network Monitor**: A comprehensive network monitoring and management tool that allows you to monitor your network in real-time and receive alerts when issues arise. It has a free version with limited features and supports Windows and Linux.

Network Analytics

Network analytics tools

- **Wireshark**: A popular and widely-used network protocol analyzer that allows you to see what's happening on your network at a microscopic level. It's available for Windows, Mac, and Linux and is free to use.

- **PRTG Network Monitor**: A comprehensive network monitoring and management tool that allows you to monitor your network in real-time and receive alerts when issues arise. It has a free version with limited features and supports Windows and Linux.

Network Analytics

Network analytics tools

- **Zabbix:** An open-source monitoring tool that allows you to monitor network performance, availability, and other metrics. It has a user-friendly interface and supports a variety of platforms, including Windows, Linux, and macOS.

- **Nagios**: A widely-used open-source network monitoring tool that allows you to monitor network services, hosts, and applications. It supports a wide range of platforms and is highly customizable.

Network Analytics

Network analytics tools

- **Nmap:** A powerful network exploration and security auditing tool that allows you to discover hosts and services on a network, as well as identify security issues. It's available for Windows, Mac, and Linux and is free to use.

- **Cisco Prime Infrastructure**: A management tool for Cisco networks that provides end-to-end visibility and control.

- **SolarWinds Network Performance Monitor**: A monitoring tool that provides real-time visibility into network performance, availability, and health.

Network Analytics

Network analytics tools

- **Splunk:** A platform for collecting, analyzing, and visualizing machine data.
- **Elasticsearch**: A search engine that can be used for log analysis, security analytics, and performance monitoring.
- **Grafana**: A platform for creating and sharing real-time dashboards for monitoring and analysis.
- **IBM QRadar**: A security information and event management (SIEM) tool that provides real-time analysis of security alerts.

Network Analytics

Importance of network analytics

Diagnostics:

- Network analytics can help in identifying and diagnosing various issues in the network, including bottlenecks, connectivity problems, and security lapses.

- By analyzing the network traffic, administrators can detect anomalies and take corrective actions before they impact network performance.

Network Analytics

Importance of network analytics

Performance optimization and capacity planning:

- Network analytics can provide insights into network traffic patterns, bandwidth utilization, and application performance.

- This information can help in optimizing the network performance and capacity planning for future growth.

Network Analytics

Importance of network analytics

Credential misuse:

- Network analytics can detect unauthorized access attempts, credential misuse, and other security threats.

- By analyzing user behavior, network administrators can identify potential security risks and take appropriate action to mitigate them.

Network Analytics

Importance of network analytics

Cloud security:

- Network analytics can help in securing cloud environments by providing visibility into cloud traffic, identifying security threats, and monitoring access to cloud resources.

Network Analytics

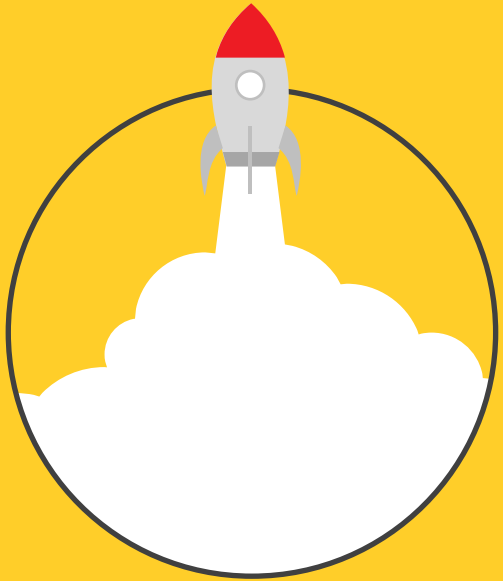
Importance of network analytics

In summary, network analytics is essential for

1. identifying and diagnosing network issues,
2. optimizing performance and capacity planning,
3. detecting security threats,
4. and securing cloud environments.

Network Analytics

Data aggregation methods



Data aggregation methods are techniques used to **collect** and **consolidate** data from multiple sources into a **unified dataset**.

Network Analytics

Data aggregation methods

Deep Packet Inspection (DPI):

1. DPI is a technique used to capture and analyze network traffic at the packet level.
2. It can be used to extract specific data elements from network traffic, such as application protocols, packet headers, and payloads.

Network Analytics

Data aggregation methods

Streaming telemetry:

1. Streaming telemetry is a method of data collection that involves the continuous streaming of data from network devices to a centralized data repository.

2. It can be used to monitor real-time network performance and detect anomalies or issues as they occur.

Network Analytics

Data aggregation methods

Context-based data collection:

1. This involves the collection of data from third-party sources, such as weather sensors or social media feeds, to provide additional context and insights into network performance.

2. This can include factors such as time of day, location, and weather conditions.

Network Analytics

Data aggregation methods

- Data validation is an important step in the data aggregation process that involves ensuring the accuracy and completeness of the data being collected.

- This can include techniques such as **data cleansing**, **data normalization**, and **data deduplication**.


Thank You