Automation Tools

- Standard automation and programming tools like Ansible, Terraform and Python are very good at the deployment of straightforward predefined, rule-based configuration and monitoring tasks.
- For example pushing an enterprise's QoS policies to all its network devices.
- This simplifies and speeds up these operations and reduces human error.

Automation Tool Limitations

- Automation tools are not so good at more complex, dynamic tasks.
- For example learning the normal traffic patterns over an entire network, recognising anomalies, and automatically taking corrective action.
- This is nearly impossible to achieve with static policies and configurations.

Traditional Security System Limitations

- Traditional IPS use signatures to inspect packets, looking for traffic patterns which match known attacks
- This does not secure against new threats or anomalies that do not match the predefined signatures
- (Traditional IPS systems often do support some anomaly detection, but they are not typically capable of analyzing huge data sets collected over time across entire networks or of predicting future patterns)

AI Artificial Intelligence Defined

- Artificial Intelligence can help with complex, dynamic network tasks.
- Cisco define it as the simulation of human-like intelligence by computers.
- Its intelligence is capable of pattern recognition, learning, reasoning, discovering meaning, problem solving and self-correction.
- ‘General Intelligence’ where a machine has the overall intelligence of a human is a hypothetical goal. Current applications are ‘Narrow AI’ which perform a specific task.
- AI is a broad term with many different usages and techniques.

Artificial Intelligence Examples

- Web search engines
- Recommendation systems eg ‘the YouTube algorithm’
- Speech interaction eg Alexa
- Autonomous vehicles
- Game play eg Deep Blue chess machine
- Creative tools eg ChatGPT

- When an application becomes commonplace enough it is often no longer thought of as ‘AI’

Machine Learning Defined

- Machine Learning is a subset of AI.
- Cisco define it as mathematical and statistical methods that enable machines to mimic intelligent human behaviour by learning from data without being explicitly programmed.
- It can analyze huge data sets, identifying patterns, relationships and anomalies. It can automatically improve its performance as it learns more.

Machine Learning Training Approaches

- Like a human, to understand the data more fully it must be ‘trained’
- Training approaches:
  - Supervised learning
  - Unsupervised learning
  - Semi-supervised learning
  - Reinforcement learning

Supervised Learning

- Supervised Machine Learning learns patterns and relationships between input and output data.
- For example it is given an image of a dog as input, and the text class of ‘Dog’ as output.
- The computer is presented with ‘labeled data’ showing example inputs and outputs.
- Once this is learned the computer can map new inputs automatically.

Supervised Learning (Cont.)

- A more complex example is a bank loading a customer dataset containing balances and credit history and which customers defaulted on which loans.
- When new customer information is input the computer can predict if they are likely to default on a potential loan as the output.

Unsupervised Learning

- Unlike supervised learning, unsupervised Machine Learning is given unlabeled data and allowed to discover patterns and insights without any explicit guidance or instruction.
- It infers its own rules to structure the information based on similarities, differences and patterns.
- It can cluster the data based on similarities, create association rules based on frequent if-then patterns, and discard the least relevant information.

Unsupervised Learning (Cont.)

- A data analyst is still required to validate the outputs. For example to classify a cluster of images as Dogs.
- Unsupervised learning can be used for network anomaly detection where it discovers patterns that are unusual in a dataset of network traffic statistics.

Semi-supervised Learning

- A small amount of labeled data in addition to unlabeled data may produce an improvement in learning accuracy.

Reinforcement Learning

- In Reinforcement learning the data is accumulated from trial-and-error.
- Data is not provided as the learning method.
- A reinforcement agent decides what to do to perform a given task and learns from its experience.
- After each action an algorithm receives feedback that helps it determine whether the choice it made was correct, neutral or incorrect.
- An example usage of Reinforcement Learning is a Chess playing machine. It can play itself to automatically learn the best move for each situation.

AI and ML in Network Operations

- Machine Learning can analyze huge sets of network related data, learn normal network patterns (baselining) and detect anomalies.
- Artificial Intelligence functions can then report on anomalies and automatically take action on them, predict future patterns and issues such as upcoming congestion, and recommend optimum settings.

Predictive AI

- Predictive AI utilizes algorithms and modelling to analyse past and current data to forecast future events and behaviours.
- Machine Learning is used to understand the data and predict what is likely to occur in the future.
- An example use is to determine maintenance cycles and predict early faults in machinery based on past events and environmental factors such as heat and vibration.

Predictive AI in Network Operations

- Predictive AI can be used in Network Operations for proactive maintenance and performance optimisation.
- AI can analyse past and current traffic patterns and anomalies, performance statistics, help tickets, maintenance history and environmental factors in order to forecast problems such as security issues, congestion and hardware failures.
- This helps network engineers optimise the network and prevent issues from occurring.

Generative AI

- Generative AI utilizes patterns and relationships learned from past data to create new outputs such as text, images, audio and video.
- Supervised learning is typically used for training. The machine is given a set of labelled data and learns to generate similar content.
- ChatGPT is a well-known example of Generative AI.
- Example usages are enhanced chat, search, language translation, and creation of marketing content, music and homework essays.

Generative AI in Network Operations

- Generative AI can be used to generate network traffic pattern simulations. This is useful to identify potential issues under different conditions and help plan for future upgrades without affecting the real network.
- It can also create optimised network settings and configurations based on current conditions, for a planned upgrade, or as a solution for an issue.
- Be careful when creating configurations or asking networking questions with general tools such as ChatGPT. They are not optimised with network data and are susceptible to ‘hallucinations’.