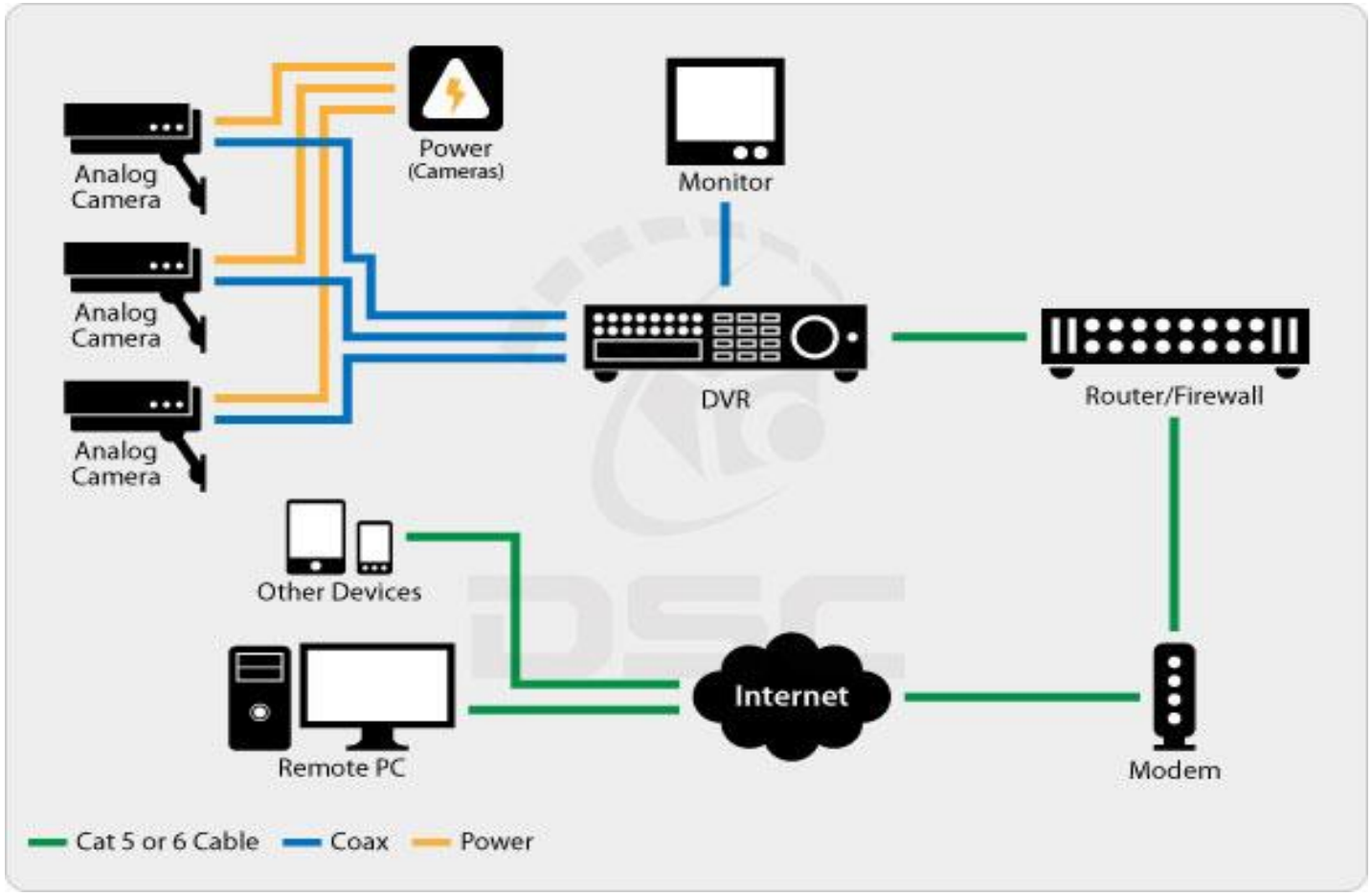
Surveillance using network device

Network surveillance

Network surveillance is the monitoring of computer activity in a network. It is usually done covertly by organizations, governments or individuals to monitor illegal activities.

A network engineer/operator, network equipment manufacturer or service provider should have the means to do surveillance tasks related to networking. Network surveillance helps governments and organizations in understanding their user base and gathering intelligence. However, at times it is perceived as a threat to network users as an invasion of privacy


Power
(Cameras)
Monitor
Analog
Camera
Analog
Camera
Analog
Camera
DVR
Router/Firewall
Other Devices
Internet
Remote PC
Modem
Cat 5 or 6 Cable
Coax
Power

- Network surveillance also provides inputs for real-time data monitoring, traffic optimization, quality of service measurements, remote protocol analysis and troubleshooting.
- One of the most important benefits of network surveillance is to help in fraud detection and location.
- From a government perspective, network surveillance allows the monitoring of threat levels, maintaining social control and helping in prevention of illegal and criminal activities.

Remote monitoring and management (RMM

- What is RMM?
- Remote monitoring and management (RMM), also known as network management or remote monitoring software, is a type of software designed to help managed IT service providers (MSPs) remotely and proactively monitor client endpoints, networks and computers. This is also now known as or referred to as remote IT management.

Functions include the ability to

- install new or updated software remotely (including patches, updates and configuration changes)
- detect new devices and automatically install the RMM agent and configure the device
- observe the behavior of the managed device and software for performance and diagnostic tasks
- perform alerting and provide reports and dashboards

Network Monitoring Techniques Your Enterprise Needs to Use

- Network monitoring tools provide IT teams with insights into their networks. These insights allow teams to analyze a network's performance, security, and efficiency, among other metrics. Monitoring tools, including network performance monitors (NPMs), use various monitoring methods to analyze the network. Most tools perform a number of different network monitoring techniques to provide users with valuable performance analysis.

- **Ping monitoring**
- Network pings are one of the oldest monitoring techniques, but it is still widely used by NPMs today. The monitoring tool sends a packet (or multiple packets) to a node or device, expecting to receive a response back. If the target node sends back an “all-clear” message, the monitor knows the node is up-and-running. However, if no response is received, it sends out more pings to get the node’s attention. If these pings still turn up nothing, the monitoring tool alerts the user. Pings are a relatively simple monitoring technique, but are still a great way for enterprises to examine if devices are currently running.

- **Log file monitoring**
- Typically, devices on a network will generate log files as they operate. These log files provide basic information that the device can report on, including any errors. While it isn't as sophisticated as other techniques, some tools monitor log files to look for device-reported troubles. Log files are simple text files that might contain keywords such as "error" or "critical" that signal a problem with the node. Monitoring tools look for these keywords and report on anything unusual.

- **SNMP monitoring**
- Most devices nowadays are compliant with SNMP, or Simple Network Management Protocol. SNMP is a device protocol that provides monitoring tools and nodes a common language to communicate with each other. The system relies on agents inside devices to provide information to network managers and monitoring tools. An SNMP manager sends out polls to devices to inquire about their current status, and devices can send traps when significant network events occur. NPMs that include SNMP monitoring have a common framework to talk to each other, centralizing and simplifying monitoring capabilities.

- **SQL query monitoring**
- To monitor databases connected to a network, monitors can utilize SQL queries. These queries ask the database to provide information on the number of data requests, transmissions, etc. Using this information, a monitor can determine if the database is performing adequately or not. Ideally, the database should be sending data across a network to accommodate for every request it receives; if the database is performing slowly, the monitoring tool can detect it and inform the network team.