

CODAN 8800 DMR Network management principals

Purpose

This document provides an overview of the principals of network management for a CODAN Digital Microwave Radio (DMR) network. The content is aimed at a non-technical reading audience.

Overview

A Network Management System (NMS) is a centrally-located PC that is used to control and monitor equipment located at remote and often not easily accessible sites.

Vendors of digital microwave radios have historically implemented their network management solutions in manufacturer-specific ways. Significant incompatibilities in software and communication methods for monitoring across the industry forces operators to maintain and support several different monitoring software packages.

There is an increasing requirement for vendors to adopt an open standard for implementing network management solutions, thus enabling operators to use a single software package to monitor their entire network. The most commonly requested standard is Simple Network Management Protocol (SNMP).

Implementing SNMP management principles enables users of DMR equipment to efficiently monitor and control the performance of their entire network from a central, convenient location.

Historical trends

The 1990s saw rapid growth in the DMR network industry. During this period, telecommunications operators realised the cost benefits that could be obtained by monitoring and controlling their transmission networks in an effective manner.

Many companies experienced problems with monitoring network performance, especially when using several different types of transmission equipment within their network. Each type of equipment had its own monitoring and control software application, with associated maintenance issues, and these applications were often incompatible with each other. These incompatibilities prevented a network being monitoring and controlled from a common network management platform.

During recent years there has been a migration towards DMRs that can be monitored and controlled by a single network management centre. This trend, coupled with similar trends within the IT industry, led to the adoption of SNMP for monitoring and control within DMR networks. This common communication protocol for network management purposes has enhanced and simplified management capabilities.

Architecture

All network management architectures use the same basic structure of central monitoring computers and remote stations. Figure 1 shows the typical architecture for a basic network containing two hops of DMR, connecting sites A to B and sites B to C. Customer access multiplexers are included at sites A and C.

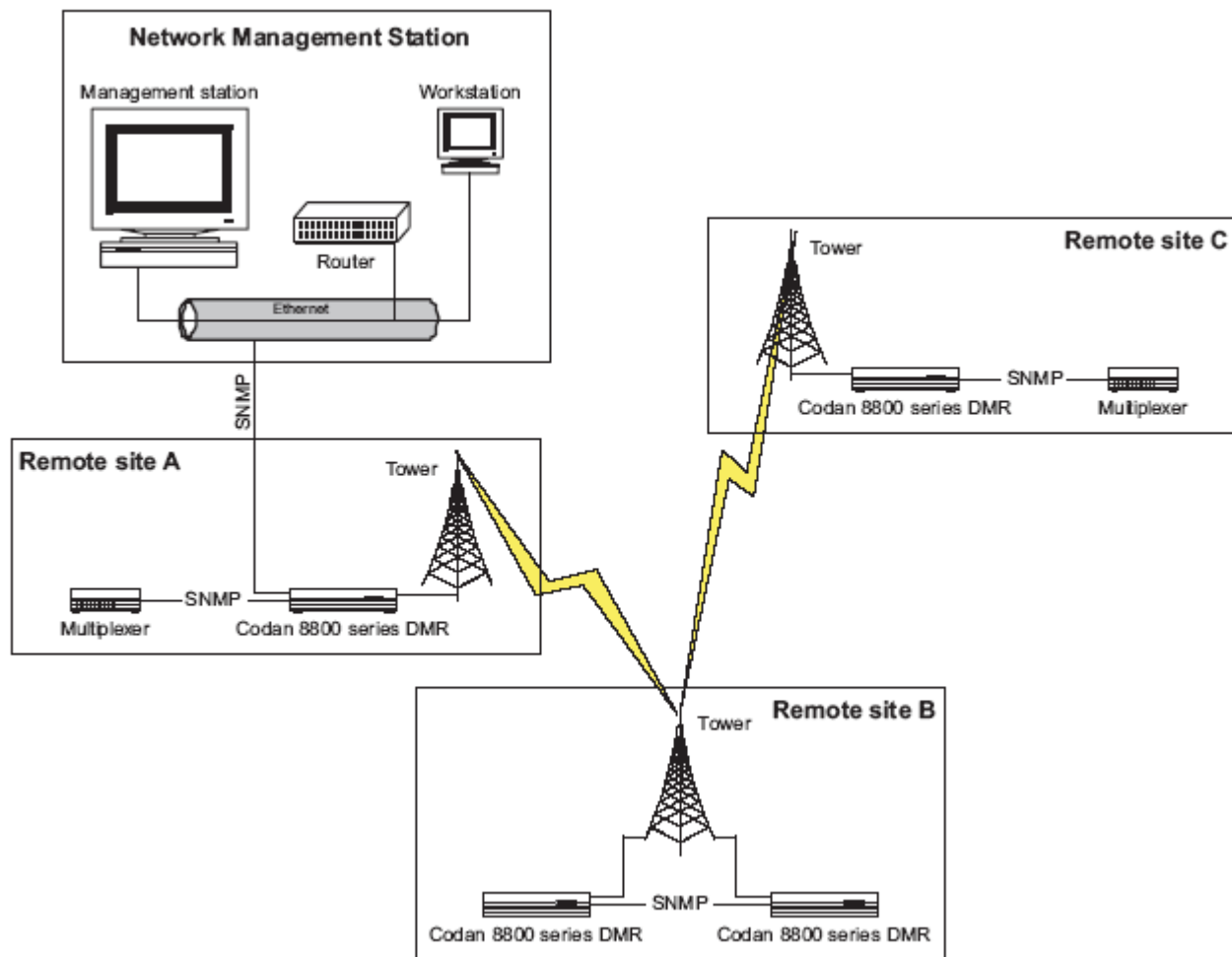


Figure 1: Codan DMR Typical network management system

All SNMP systems consist of three main parts:

- management station
- management agent
- Management Information Database (MIB)

The management station consists of a management PC running a software package to provide the interface between the human network manager and the network management system.

The devices at remote stations run software (management agent) located inside each device to be managed. The agent enables the device to send alerts, known as traps, to the central monitoring PC when a pre-determined event occurs. The events include alarms or user-defined thresholds being passed, and are determined either by the device itself or are configurable by the user. Agents also compile information about the managed devices where they reside, and then store this information locally in a MIB.

The MIB is a database file that the manager and agent use to locate, retrieve and control data relating to the managed device. MIBs come in two types:

- Public MIBs, which are used for items that are not application-specific (for example, Transmission Control Protocol/Internet Protocol (TCP/IP) address locations). Public MIBs are supplied with the agent and manager.
- Private MIBs, which are used for application/equipment-specific reasons (for example, configuration and performance data for the 8800 series DMR). Private MIBs are supplied with the agent and as data files to be loaded onto the management station.

Objectives of network management

There are four key objectives for successful implementation of an NMS. These objectives are: configuration management, performance management, fault management and security management.

Configuration management

Configuration management monitors and controls device configuration so that the operation of various types of equipment can be tracked and managed. The ability to configure remote devices is essential.

As an example, when additional DMRs are added to the network, it may become necessary to change the operating frequency of a remote microwave link, or to change the data speed of one of the digital ports. Configuration management through an NMS enables these changes to be carried out without visiting the remote site.

Performance management

Performance management measures network statistical information. Examples of DMR performance parameters that might be measured include bit error rate (BER) performance, receive signal level, Ethernet utilisation, and the occurrence of hot standby switching.

Performance management involves:

- gathering performance data on parameters of interest to the management station
- analysing the data to determine normal minimum acceptable levels
- setting appropriate performance thresholds for each parameter so that exceeding these thresholds indicates a network problem worthy of attention

Fault management

Fault management detects, logs, notifies users of, and if possible fixes problems to keep devices running effectively. Faults can cause downtime or unacceptable network degradation, therefore fault management is perhaps the most important of the network management objectives. Fault management can involve analysing the symptoms, isolating the problem, providing a fix, and testing the fix.

Security management

Security management provides protection for your DMR network.

Security management involves:

- controlling access to network resources according to operator-determined requirements so that the network cannot be sabotaged (intentionally or accidentally)
- restricting access to sensitive information by those without appropriate authorisation
- monitoring operators logging on to a DMR within the network

Conclusion

Network management is a necessary feature for the modern telecommunications network. SNMP is a universally-accepted protocol with the ability to manage many different equipment and manufacturer types.

Digital Microwave Radio | Network Management

http://digital-microwave-radio.at-communication.com/en/at/digital_microwave_radio_8800_network.html