

INTRODUCTION

This sequence of Web pages is a discussion of **Annex J** to **ANSI/ASHRAE 135-1995, BACnet™**. The annex, **BACnet/IP**, describes how BACnet networks may be formed from collections of devices that use the TCP/IP family of protocols for their communication. Where you see text that is indented and bold, it is text from the annex and will be followed by commentary

Here are the basic provisions of the BACnet/IP specification:

1. The concept of a BACnet network made up of one or more IP subnets is described.
2. Management of broadcasts of all types (local, remote, global), and thereby the use of BACnet unconfirmed services, is specified both within and between BACnet/IP and non-BACnet/IP, i.e., traditional, BACnet networks.
3. Broadcast management is accomplished by defining the capabilities of a new device called a BACnet Broadcast Management Device (BBMD). Alternatively, IP Multicast may be used.
4. BACnet/IP communication is implemented by defining a new protocol layer called the "BACnet Virtual Link Layer" or BVLL. The advantages are many: this approach is readily extensible to other, future transport mechanisms such as IPv6, ATM, Sonet, and so on. Second, the concept of defining an extensible mechanism for peer-to-peer management of BACnet messages - beyond merely solving the broadcast limitations of the Internet - means that other manipulations, such as encryption/decryption and compression/decompression can be performed outside of the process of generating BACnet APDU/NPDUs, i.e., without altering the existing standard.
5. Provision is made for "foreign" devices to join BACnet/IP networks and thus, potentially, a BACnet internetwork. This part of the specification addresses, among other things, the requirements for remote workstation access, including access via SLIP or PPP.
6. Routing between BACnet/IP and non-BACnet/IP networks is specified, including the case where IP and non-IP BACnet devices reside on the same LAN.
7. Routing between multiple BACnet/IP networks is specified.

This presentation will explain the philosophy behind the BACnet/IP proposal as well as many details that will hopefully become clear as a result of these largely pictorial pages

A note about security...

There is little discussion of security in this presentation. We have assumed that all nodes are "trusted." Security will obviously be an important future consideration. For now assume that all devices are sitting behind a firewall that does packet filtering and the environment has well-implemented restrictions on the software that can run inside the firewall