9.5 Conclusion

Our study of network management, and indeed of all of networking, is now complete!

In this final chapter on network management, we began by motivating the need for providing appropriate tools for the network administrator—the person whose job it is to keep the network "up and running"—for monitoring, testing, polling, configuring, analyzing, evaluating, and controlling the operation of the network. Our analogies with the management of complex systems such as power plants, airplanes, and human organization helped motivate this need. We saw that the architecture of network management systems revolves around five key components: (1) a network manager, (2) a set of managed remote (from the network manager) devices, (3) the Management Information Bases (MIBs) at these devices, containing data about the devices' status and operation, (4) remote agents that report MIB information and take action under the control of the network manager, and (5) a protocol for communication between the network manager and the remote devices.

We then delved into the details of the Internet-Standard Management Framework, and the SNMP protocol in particular. We saw how SNMP instantiates the five key components of a network management architecture, and we spent considerable time examining MIB objects, the SMI—the data definition language for specifying MIBs, and the SNMP protocol itself. Noting that the SMI and ASN.1 are inextricably tied together, and that ASN.1 plays a key role in the presentation layer in the ISO/OSI seven-layer reference model, we then briefly examined ASN.1. Perhaps more important than the details of ASN.1 itself was the noted need to provide for translation between machine-specific data formats in a network. While some network architectures explicitly acknowledge the importance of this service by having a presentation layer, this layer is absent in the Internet protocol stack.

It is also worth noting that there are many topics in network management that we chose *not* to cover—topics such as fault identification and management, proactive anomaly detection, alarm correlation, and the larger issues of service management (for example, as opposed to network management). While important, these topics would form a text in their own right, and we refer the reader to the references noted in Section 9.1.

Homework Problems and Questions

Chapter 9 Review Questions

SECTION 9.1

R1. Why would a network manager benefit from having network management tools? Describe five scenarios.

R2. What are the five areas of network management defined by the ISO?

R3. What is the difference between network management and service management?

SECTION 9.2

R4. Define the following terms: managing entity, managed device, management agent, MIB, network management protocol.

SECTION 9.3

R5. What is the role of the SMI in network management?

R6. What is an important difference between a request-response message and a trap message in SNMP?

R7. What are the seven message types used in SNMP?

R8. What is meant by an "SNMP engine"?

SECTION 9.4

R9. What is the purpose of the ASN.1 object identifier tree?

R10. What is the role of ASN.1 in the ISO/OSI reference model's presentation layer?

R11. Does the Internet have a presentation layer? If not, how are concerns about differences in machine architectures—for example, the different representation of integers on different machines—addressed?

R12. What is meant by TLV encoding?

Problems

P1. Consider the two ways in which communication occurs between a managing entity and a managed device: request-response mode and trapping. What are the pros and cons of these two approaches, in terms of (1) overhead, (2) notification time when exceptional events occur, and (3) robustness with respect to lost messages between the managing entity and the device?

P2. In Section 9.3 we saw that it was preferable to transport SNMP messages in unreliable UDP datagrams. Why do you think the designers of SNMP chose UDP rather than TCP as the transport protocol of choice for SNMP?

P3. What is the ASN.1 object identifier for the ICMP protocol (see Figure 9.3)?

P4. Suppose you worked for a US-based company that wanted to develop its own MIB for managing a product line. Where in the object identifier tree (Figure 9.3) would it be registered? (*Hint:* You'll have to do some digging through RFCs or other documents to answer this question.)

P5. Recall from Section 9.3.2 that a private company (enterprise) can create its own MIB variables under the private branch 1.3.6.4. Suppose that IBM wanted to create a MIB for its Web server software. What would be the next OID qualifier after 1.3.6.1.4? (In order to answer this question, you will need to consult [IANA 2009b]). Search the Web and see if you can find out whether such a MIB exists for an IBM server.

P6. Why do you think the length precedes the value in a TLV encoding (rather than the length following the value)?

P7. Consider Figure 9.9. What would be the BER encoding of {`weight, 165`} {`lastname, "Michael"`}?

P8. Consider Figure 9.9. What would be the BER encoding of {`weight, 145`} {`lastname, "Sridhar"`}?