INSTRUCTOR'S MANUAL

BUSINESS DATA NETWORKS AND SECURITY, 9TH EDITION

RAYMOND R. PANKO
JULIA L. PANKO

PRENTICE-HALL, 2013

Control-Click on a link to follow it.

READ THIS FIRST

It is important to understand that this book is not intended to be covered front-to-back in its entirety. The 11 core chapters (excluding the hands-on chapters and the modules) form a complete course in networking. If you cover all 11 chapters, you are likely to have a week or so free for other things, such as the hands-on chapters that follow some chapters, one of the four modules at the end, or a few things those stupid authors should have put in and you have to add yourself. However, *there is not time to cover the entire book*, including all hands-on chapters and all four modules, in a normal one-semester or one-quarter course.

> There is not time to cover the entire book, including all hands-on chapters and all four modules, in a normal one-semester or one-quarter course.

I teach courses on a semester basis. Each of the 11 core chapters takes me about three hours to cover. This is one semester week in a three-unit course. Module C is about equally long. (Modules A, B, and D are shorter.) Hands-on exercises vary in time from about 15 minutes to a class.

You can also shorten the chapters. The easiest way to do this is to skip boxed material which is somewhat secondary. (The box on decibels is particularly long.)

I cover a chapter, and then spend the first 20 minutes of the next class going over parts of the assigned homework students feel unsure about and all of the end-of-chapter questions. I then cover the start of the next chapter the rest of that day and all of the next day.

My suggestion, frankly, is that the first time you teach the book, stick with the 11 core chapters and one or two hands-on exercises.

TEACHING THE CHAPTERS

TEACHING THE BOOK IN GENERAL

POWERPOINT PRESENTATIONS

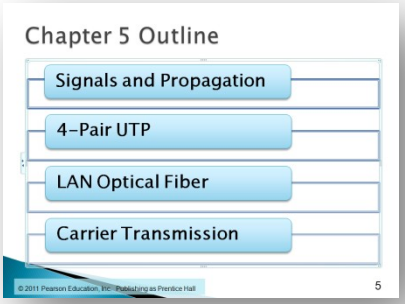
The chapter and module PowerPoint presentations are full lectures—not just "a few selected slides."

In the book, nearly all concepts are illustrated in the figures, and the figures are the basis for the PowerPoint presentations. The figures are somewhat adjusted for the PowerPoint presentations.

- First, the font size is increased so that you can print six slides per page and still read them.
- Second, more complex figures are presented as a series of slides that build these figures in steps.
- Third, central concepts (CEPTs) that are critical for understanding networking are marked. You probably want to give them special emphasis.
- Fourth, material that is difficult for some students is also marked. You probably want to slow down for this material. Make sure that their eyes are open, get them off their phones, and so forth.

Central Concept (CEPT)	Difficult Material
	

PowerPoint presentations are divided into sections that are marked in a reasonably consistent way. (Chapter 3 used a different section organization built around the plan/protect/respond security management cycle, and the modules do not all use it.)



QUESTION-FOCUSED SUPPORT

There are Test Your Understanding questions after subsections in each chapter. Students should read a section and then answer the questions before going on.

There are meaty End-of-Chapter questions that require students to think about what they have learned in the chapter.

The answer keys (not to be given to students) give the teacher answers for all questions in the chapter.

Importantly, in the test item files, (multiple choice/true-false), all questions are tied to specific questions in the chapter. So if you assign specific textbook questions students are responsible for, you can select exam questions to reflect them.

All multiple choice and true-false questions in the test item file (TIF) are tied to specific questions in the chapter. So if you assign specific textbook questions students are responsible for, you can select exam questions to reflect them.

TEACHING DIFFERENT KINDS OF COURSES

As noted earlier, this book has 11 core chapters. These can form a complete course.

Junior and Senior Courses in Information Systems Programs

With courses for juniors and seniors, covering the 11 core chapters (including “a” chapters that are case studies) will probably leave you with one or two semester weeks free. As noted earlier, this leaves time for hands-on activities (discussed earlier), additional TCP/IP material (or other material in the advanced modules), a term project, or whatever you wish to cover. However, the entire book should not be covered in a single term.

Community College Courses

For freshman and sophomore courses in community colleges, it is good practice to stay with the 11 core chapters, going over chapter questions in class. If you want to do hands-on material, it is advisable to cut some material from the core chapters.

Graduate Courses

Graduate courses tend to look a lot like junior and senior level courses, but with greater depth. More focus can be placed on end-of-chapter questions and novel hands-on exercises, such as OPNET simulations. It is also typical to have a term project.

TEACHING CHAPTER 1: WELCOME TO THE CLOUD

Role in the Book

The growing complexity of networking requires four introductory chapters. The concepts introduced in this chapter will be reinforced throughout the book.

Chapter 1 covers general concepts and principles we will see throughout the book.

Chapter 2 covers standards concepts and architectures, Chapter 3 covers network security, and Chapter 4 covers network management.

After these four introductory chapters, we move up through the layers, applying concepts in the first four chapters to switched Ethernet networks, wireless LANs, internets, WANs, and applications.

Flow of the Material

The chapter begins with examples of how people use applications "in the cloud" today.

It then introduces basic network terminology.

It next discusses circuit switching and packet switching. It presents packet switching historically, in the context of the ARPANET.

Next comes the emergence of internetworking and the Internet.

The chapter closes with the components in a small home network to make the material in the chapter more concrete.

Changes from the Previous Edition

The opening material has been changed to focus on cloud applications.

The final part has been shortened. There is no longer a discussion of LANs versus WANs. Students already know the basic distinction from earlier classes, and it seemed best to move this material to Chapter 5 (the start of LAN material) and Chapter 10 (the new chapter on WANs).

Central Concept

In the definition of networking, a host is defined as any device connected to a network—servers, client PCs, smart phones, and so forth.

The chapter includes a discussion of the five layers of network operations and standards: physical, data link, internet, transport, and application.

Hard Parts

Some students have a difficult time appreciating why packet switching is superior to circuit switching for bursty data.

Many students have a difficult time distinguishing between packets and frames, switches and routers, and data links and packets. The chapter shows how internetworking evolved historically out of single networks and that Cerf and Kahn had to define a second level of networking in which concepts were duplicated at both layers.

Teaching this Chapter

If you can bring in any Internet memorabilia props, that's kind of fun.

Also, it helps to bring in a big switch, a big router, UTP, and home networking equipment at appropriate times in the chapter.

I often start with a discussion asking whether networking means the same thing as the Internet, when was the Internet created, who pays for the Internet, and so forth. We then cover these questions in the chapter lecture.

I assign Chapter 1a as homework. I spend a good deal of time going over student answers. (If I don't, students stop taking hands-on exercises seriously.)

Having students use Google docs or Microsoft Office Web Apps is a good way for them to appreciate cloud computing. Although cloud computing is not covered until Chapter 11, you might start the term having them work in group projects with these tools and use these tools throughout the term. In general, these tools are better for viewing documents than for creating them, so they should be able to work with existing personal productivity tools.

Chapter 1a: Hands-On Networking Tools

Chapter 1a has a number of hands-on exercises to help students "burn internetworking concepts into mental ROM." They learn how to convert 32-bit IP addresses to dotted decimal notation. Using web-based tools, they learn how to check their Internet connection speed. Students go to the Windows command line to use ping, tracert, and nslookup for DNS. They also learn to look up RFCs—specifically, a joke RFC regarding using carrier pigeons to carry packets. Students enjoy this chapter, and it makes the concepts in Chapter 1 more concrete.

CHAPTER 1: WELCOME TO THE CLOUD

Note: Page numbers are indicated by square brackets [ ].

TEST YOUR UNDERSTANDING QUESTIONS

1. a) Why do you think wireless is such a big concern today in networking and security? (In this book, "do you think" questions require you to go beyond what is in the text. You may not be able to answer them perfectly, but try hard because they are good learning opportunities.) [1–4]

   Some talking points:

   Most network implementations today are wireless.

   Wireless transmission is more risky because adversaries can easily intercept signals.

Wireless propagation is less predictable than wired transmission

Wireless standards and products are maturing rapidly.

b) Distinguish between cloud data storage and synchronization on the one hand and cloud software service on the other. [2–4]

Some talking points:

Cloud data storage and synchronization is concerned only with data handling.

Cloud software service makes applications available to users.

c) What do you think are the advantages of each? [2–4]

Some talking points:

Data service is simpler and therefore more manageable.

Providing applications is a good way to increase value.

d) What do you think are their disadvantages? [2–4]

Some talking points:

They represent major security risks.

Services are immature and therefore difficult and costly to use from the labor viewpoint.

e) Why do you think the bring your own device (BYOD) revolution has made networking more difficult? List several issues. [1–4]

Some talking points:

There is great device diversity and no standardization of devices.

Security on BYOD devices is immature to nonexistent.

Employees typically own their devices, so control over them is difficult.

Employees typically mix personal and business data and applications.

Employees do not understand security issues well.

There is limited management application software for managing BYOD devices.

There is no consensus on how to manage BYOD devices.

2. Go to YouTube and watch “A Day Made of Glass” by the Corning Corporation. List new ways of displaying information shown in the video. [No Page Numbers]

Walls and mirrors

Table tops

Devices such as refrigerators and stoves

Traffic kiosks

In-store displays

Images can be moved among these devices

3. a) What information could Claire learn about individual access points? [5–6]

Names (SSIDs)

Signal strengths

Ethernet address (BSSIDs)

Security standards in use

b) Distinguish between SSIDs and BSSIDs. [5]

The SSID is the name of the access point and network (FBP).

The BSSID is the access point's (Ethernet) address.

c) What is a rogue access point? [6]

An access point set up by an individual employee or department without authorization.

d) Why do you think rogue access points are dangerous? [6]

Some talking points:

They may have poor security, allowing attackers to get in without going through the site's firewall.

They may interfere with the operation of legitimate access points.

e) Why is centralized wireless management highly desirable compared to "management by walking around" as Claire does today? [6]

She will not have to walk around to find transmission problems.

It will identify rogue access points and access points outside the building automatically.

She can remotely diagnose problems and make changes.

She can dynamically adjust access point power to special conditions.

4. a) List major wireless LAN security issues. [7–9]

The need to create security policies for mobile devices

Maturity of security on devices is improving, but new problems constantly appear

Diversity of device software

Pace of change in technology

Physical loss of mobile devices

Rogue access points are a problem

b) Why is BYOD security so difficult today? [7]

Immaturity of product security

High diversity among products

Rapid pace of change

5. Why does this book combine networking and security? [7–8]

The two are inseparable today at every stage of the network life cycle.

Networking people constantly run into security issues.

Security people find that many of their problems are concerned with networks.

6. a) Give the book's definition of network. [8]

As a working definition, a network is a system that permits applications on different hosts to work together.

b) What is a networked application? [9]

Networked applications are applications that require networks to work.

c) What are Web 2.0 applications? [9]

In Web 2.0 applications, users supply the content.

d) What are social media applications? [9]

These are applications that facilitate the creation and maintenance of group relationships.

e) What is a host? [10]

A host is any device attached to a network.

f) Is your laptop PC or desktop PC a host? [9–10]

Yes, if it is connected to a network.

g) Is a smartphone a host? [9–10]

Yes

h) Why is the network core shown as a cloud? [10]

To emphasize that the user does not have to look inside the cloud to see how it works.

i) Why may the user need to know more about his or her access link than about the network cloud? [10–11]

If the user needs to take any action regarding the network, it is likely to be regarding the access link.

Users may have to plug in access link technology, configure it, and troubleshoot simple problems.

7. a) Are network speeds usually measured in bits per second or bytes per second? [13]

Bits per second

b) How many bits per second (without a metric prefix) is 20 kbps? Use commas. [13]

20,000 bps

c) How many bits per second (without a metric prefix) is 7 Mbps? Use commas. [13]

7,000,000 bps

d) How many bits per second (without a metric prefix) is 320 kbps? Use commas. [13]

320,000 bps

e) Is the metric prefix for kilo k or K? [13]

k

f) Express 27,560 bps with a metric prefix. [13]

27.56 kbps

8. a) Why is paying for a transmission line by the minute not too bad for voice conversations? [15]

One person or the other is talking most of the time, so there is not a huge amount of unused bandwidth being wasted.

b) For what two reasons is paying for a transmission line by the minute bad for data transmissions? [15]

Data transmission is bursty, with short bursts of traffic separated by long silences. A great deal of paid-for bandwidth is wasted.

9. a) In packet switching, what does the source host do? [16–17]

   In packet switching, the source host fragments the application message into many smaller pieces called packets. It submits these packets to the network.

   b) About how long is a packet? [16]

   About 100 bytes long

   c) Why is fragmentation done? [17]

   Packet switching saves money by multiplexing multiple conversations over expensive circuits.

   d) Where is reassembly done? [16]

   On the destination host

   e) What are the two benefits of multiplexing? [17]

   It reduces costs.

   If there is an error in a packet, only that packet has to be resent—not the entire application message.

   f) When a packet switch receives a packet, what decision does it make? [17]

   It makes a forwarding decision—deciding which port to send the packet back out.

   g) Do packet switches know a packet's entire path through a network? [18]

   No

   h) In Figure 1-14, if Packet Switch A receives a packet addressed to Destination Host W, where will it send the packet?

   Packet Switch C

10. a) In Figure 1-15, how many physical links are there between the source host and the destination host along the indicated data link? [20]

    5

    b) How many data links are there between the source host and the destination host? [20]

    1 (by definition)

    c) If a packet passes through eight switches between the source and destination hosts, how many physical links will there be? (Careful!) [19-20]

    9 (Draw the picture. There is always one more link than switches.)

    d) How many data links will there be? [19-20]

    1 (by definition)

11. a) On the ARPANET, explain the functions of IMPs. [20]

    They fragment application messages and act as packet switches.

    b) How is this like what packet switches do today? [20]

They forward packets.

c) How is it more than packet switches do today? [20]

They also fragment application messages. This is done by hosts today, rather than packet switches.

12. a) What organization sets Internet standards today? [22]

The Internet Engineering Task Force (IETF)

b) What does the IETF call its standards? [21]

Requests for comments (RFCs)

13. a) How did Ray Tomlinson extend e-mail? [22]

Previously, e-mail was sent only between users on the same server host.

Tomlinson extended e-mail to be sent between users on different server hosts.

b) How did he change e-mail addresses? [22]

Previously, e-mail addresses had been user account names on the host.

He also needed to add the host on which the account resided to the address.

His final address was the account name, an @ sign, and the hostname.

14. What problem did Bob Kahn face? [23]

He was supporting several networks, and users on one network could not communicate with hosts on other networks.

15. a) What device connects different networks into an internet? [23]

A router

b) What is the old name for this device? [23]

Gateway

16. a) Distinguish between internet with a lowercase *i* and Internet with an uppercase *I*. [25]

Lowercase: an internet and the internet layer (except at the beginning of a sentence)

Uppercase: the global Internet

b) Why are many networking concepts duplicated in switched networks and internets? [25]

Individual networks already existed. They had different technologies and addressing schemes. The only way to connect their users was to add a second level of networking, including messages, forwarding devices, and end-to-end paths.

c) What are the two levels of addresses? [25]

Single network addresses (at the data link layer)

Internet addresses (IP addresses) at the internet layer

d) How long are IP addresses? [25-26]

Initially, in IPv4, 32 bits

Later, in IPv6, 128 bits

e) How are IPv4 addresses usually expressed for humans? [25-26]

IPv4 addresses are expressed in dotted decimal notation for human reading.

f) Distinguish between packets and frames. [26]

Packets at the data link layer are called frames, and packets at the internet layer are called packets.

g) A host transmits a packet that travels through 47 networks. How many packets will be there along the route? [26]

One

h) How many frames will be there along the route? [26]

47

i) Are frames carried inside packets? [26]

No, packets are carried inside frames.

j) Distinguish between switches and routers. [27]

Switches are forwarding devices for frames at the data link layer.

Routers are forwarding devices for packets at the internet layer.

k) Distinguish between physical links, data links, and routes. [27]

A physical link connects adjacent devices in a single network.

A data link is the path a frame takes through a single network.

A route is the path a frame takes through an internet.

l) Distinguish between what happens at the internet and transport layers. [27-28]

The internet layer forwards a packet across routers from the source host to the destination host. The internet layer also governs packet organization.

The transport layer fragments and defragments application messages. It also checks for errors.

m) Do IPv4, IPv6, or both use dotted decimal notation for human reading? [25-26]

No

n) Why are application layer standards needed? [28]

So that application programs can work together.

o) List the numbers and names of the five layers. [29]

5 Application

4. Transport

3. Internet

2. Data Link

1. Physical

17. a) What are the roles of the Internet Protocol? [30]

The Internet Protocol deals with addresses and functionality for routers to move packets across an internet.

b) What are the roles of the Transmission Control Protocol? [30]

It places packets in order, corrects errors, and reduces the likelihood of congestion.

It also does fragmentation and defragmentation.

c) What are the limitations of the User Datagram Protocol? [30]

It cannot do error handling.

Application messages must fit into a single UDP datagram.

d) Why is UDP used sometimes? [30]

Requires less processing burden on the hosts

Creates less traffic burden on the network

e) What is TCP/IP? [31]

TCP/IP is a family of standards including IP, TCP, UDP, and many other standards.

18. a) In what sense is January 1, 1983, the birthday of the Internet? [31]

On that day, NCP was ended and all hosts had to follow TCP/IP.

b) In what sense is it not? [31]

Most systems were already using TCP/IP anyway.

19. a) What was the Acceptable Use Policy in place on the Internet before 1995? [31]

The NSF ran the backbone. It forbade the use of commercial activities through the AUP.

b) Why did commercial activities on the Internet become acceptable in 1995? [31]

The government stopped paying for Internet transmission, so its restrictions on the Internet's use ceased to exist. The Acceptable Use Policy was gone.

c) What do we call the carriers that provide Internet service? [31]

Internet service providers [ISPs]

d) Why do they need to be interconnected? [31]

Two hosts that need to communicate over the Internet may be on different ISPs. The ISPs need to be interconnected to carry such traffic.

e) At what locations do ISPs interconnect? [31]

Network access points (NAPs)

20. a) Why do servers need static IP addresses? [33]

So that client hosts can know how to find them.

b) What protocol provides a client PC with its dynamic IP address? [33]

The Dynamic Host Configuration Protocol (DHCP)

c) What other configuration information does this protocol provide? [33]

Configuration information also includes the IP addresses of local Domain Name System (DNS) servers, which we will see next. It includes other information such as a subnet address mask, which we will see later in this book.

d) Why should PCs get their configuration information dynamically instead of manually? [34]

With DHCP, every client PC automatically gets hot fresh information every time it boots up. If configuration information changes, all client PCs will be updated automatically. With manual configuration, every change in basic configuration information would require manual changes on each client. This would be very expensive.

21. a) To send packets to a target host, what must the source host know? [34]

The IP address of the target host.

b) If the source host knows the host name of the target host, how can it get the target host's IP address? [34]

It sends a DNS request message to a DNS server. This message contains the host name of the target host and requests the IP address of the target host.

The DNS server sends back a DNS response message containing the IP address of the target host (or an error message explaining why it failed to find the requested IP address).

22. Both DHCP servers and DNS servers send a host an IP address. These are the IP addresses of what hosts?

This is an important question that helps students distinguish between these two types of servers.

DHCP servers give a client an IP address for the client to use as its own.

DNS servers give a client the IP address of a target host, to which the client host wishes to send packets.

23. a) List the hardware elements in the small home network described in this section. [35–37]

Broadband modem

Wireless access router

Client PCs (and other client devices)

Printer

4-Pair UTP wiring

b) For wired connections, what transmission medium is used? [36]

4-pair UTP.

c) What is its connector standard? [36]

RJ-45

d) What is the standard for wireless PCs and printers to connect to a wireless access point? [36]

802.11

e) What are the five hardware functions in a wireless access router? [37]

Router

Ethernet switch

Wireless access point (if included)

DHCP server

Network Address Translation (NAT)

f) Why is the DHCP function necessary? [37]

So that hosts on the home networks can have individual IP addresses. The ISP gives only a single ISP address to the access router.

g) Why is NAT necessary? [37]

So that transmissions to and from the Internet by different internal devices can be sent from and to the correct device.

h) What three services does this network provide to the desktop PC and the wireless tablet? [37-38]

Shared Internet access

File sharing

Printer sharing

i) Which devices need to be configured? (List them.) [38]

Each client PC

The printer

The remote access router

END-OF-CHAPTER QUESTIONS

Thought Questions

1. a) In Figure 1-15, when Host X transmits a packet along the data link shown, how many physical links are there along the data link shown?

   5

   b) How many data links? [20]

   1

2. a) In Figure 1-20, how many physical links, data links, and routes are there along the way when Host A sends a packet to Host B?

   Physical links: 7

   Data links: 3

   Routes: 1

   b) When Host E sends to Host C? (Assume that hops will be minimized across switches and routers.)

   Physical links: 8

   Data links: 3

   Routes: 1

c) When Host D sends to Host E?

Physical links: 3

Data links: 1

Routes: 1

3. In a certain network, there are nine routers between Host R and Host S. a) How many data links will there be along the way when Host R transmits a packet to Host S? (Hint: Draw a picture.)

10

b) How many routes?

1

c) How many frames?

10

4. Why does it make sense to make only the transport layer reliable? This is not a simple question.

First, error correction has to be done only on the source and destination hosts—not on each router along the way.

Second, it is directly beneath the application layer, so wherever errors occur, the application program gets clean data.

5. a) What does it mean that data transmission is bursty?

There are brief transmission bursts separated by long silences.

b) Why is burstiness bad if you pay for a transmission line by the minute?

You will be paying for capacity you are not using.

6. What layer fragments application messages so that each fragment can fit inside an individual packet?

The transport layer

Case Study

1. A friend of yours wishes to open a small business. She will sell microwave slow cookers. She wishes to operate out of her house in a nice residential area. She is thinking of using a wireless LAN to connect her four PCs. What problems is she likely to run into? Explain each as well as you can. Your explanation should be directed to her, not to your teacher. This is not a trivial problem.

Student answers will vary. The goal of this question is not to get specific answers but to help students think through the matter.

She will need to purchase cable modem service or DSL service with sufficient speed.

She will need to have a wireless access router.

She will have to configure the router and the individual PCs.

<She should turn on security.>

CHAPTER 1A: HANDS-ON:

TEST YOUR UNDERSTANDING QUESTIONS

1. a) What is 11001010 in decimal? [43–44]

   202

   b) Express the following IP address in binary: 128.171.17.13. (*Hint:* 128 is 10000000. Put spaces between each group of 8 bits.) [43-44]

   10000000 10101011 00010001 00001101

   c) Convert the following address in binary to dotted decimal notation: 11110000 10101010 00001111 11100011. (Spaces are added between bytes to make reading easier.) (*Hint:* 11110000 is 240 in decimal.) [43-44]

   240.170.15.227

2. a) What kind of connection do you have (telephone modem, cable modem, LAN, etc.)? [44]

   Student answers will vary.

   b) What site did you use for your first test? [44]

   Student answers will vary.

   c) What did you learn? [44]

   Student answers will vary.

   d) What site did you use for your second test? [44]

   Student answers will vary.

   e) Did you get different results? [44]

   Student answers will vary.

3. Go to the command line. Clear the screen. [45]

   There is no answer to this part.

4. Use ipconfig/all or winipconfig. a) What is your computer's IP address? [45]

   Student answers will vary.

   b) What is its Ethernet address? [45]

   Student answers will vary.

   c) What is your default router (gateway)? [45]

   Student answers will vary.

   d) What are the IP addresses of your DNS hosts? [45]

   Student answers will vary.

e) What is the IP address of your DHCP server? [45]

Student answers will vary.

f) When you get a dynamic IP address, you are given a lease specifying how long you may use it. What is the starting time of your lease and the ending time? [45]

Student answers will vary.

5. Ping a host whose name you know and that you use frequently. What is the latency? If this process does not work because the host is behind a firewall, try pinging other hosts until you succeed. [45]

Student answers will vary.

6. Ping 127.0.0.1. Did it succeed?

It should succeed, or the student has no Internet connection.

7. Do a tracert on a host whose name you know and that you use frequently. You can stop the tracert process by hitting Control-C. [45]

a) What is the latency to the destination host? [45]

Student answers will vary.

b) How many routers are there between you and the destination host? If this does not work because the host is behind a firewall, try reaching other hosts until you succeed. [45]

Student answers will vary.

8. Distinguish between the information that ping provides and the data that tracert provides. [45]

Ping determines if another host is reachable and provides latency to a destination host.

Tracert does this too; in addition, it identifies each router along the way and gives the latency to each router.

9. Find the IP address for Microsoft.com and Apple.com. [46]

These vary over time. In addition, each has multiple webservers, so different students will get different answers.

10. a) Look up RFC 1149. [46]

There is no answer to this part.

b) In layperson's terms, what does this RFC specify? [46]

RFC1149 is the standard for the transmission of IP datagrams on Avian Carriers—in other words, using carrier pigeons to carry packets.

c) What are its sections? (This is a serious question. You should learn how RFCs are structured.) [46]

Title

RFC Number, Date

Status of this Memo

Overview and Rational

Frame Format

Security Considerations

Author's Address

d) On what day was it created?

RFC1149 was created on April Fool’s Day in 1990, and its latest edition was created nine years later on the same day (1 April 1999).