IP Security Module for VITELS

Computer Science Project

done by:
Thomas Spreng
spreng@iam.unibe.ch

head:
Prof. Torsten Braun

assisted by:
Marc-Alain Steinemann

Computer Networks and Distributed Systems (RVS),
Institute of Computer Science and Applied Mathematics (IAM),
University of Berne.

2002,2003

Contents

List of Figures

1 Abstract

The goal of this student project was to create an “IP Security” module for the WebCT based VITELS course. This course is used by the lecture “Praktikum Computernetze” which is a hands-on training for IP based networks. Some prework was already done by a related module that was used in the previous years before the whole lecture was designed as an online course.

2 Introduction

Back in the year 2001 the lecture “Praktikum Computernetze” was designed as a laboratory where the students worked together and had physical access to all computers and routers. The lecture was split into several parts which covered a different subjects. One of them was establishing a virtual private network between two routers. After the year 2001 the whole lecture was redesigned and it turned into a online course using WebCT learning software. Like in the past the lecture was split into different modules. This student project was about creating a module called “IP Security”. All the material from the old lecture could be used for this and actually the new module was sort of an “enchanced” version of the old VPN part.

3 Concept

The “IP Security” module consists of several parts that should help the participants to understand the theory and to solve the practical exercise. After a little introduction the user is directed to the theoretical part. It gives some in-depth insight into security related topics concerning the internet protocol and virtual private networks. This section tries to impart some theoretical knowledge about what will be the subject during the hands-on part. It ends with a collection of java applets that were developped by regular students in a related lecture. This adds a graphical and animated aspect to the theory.

Then a part with links to external theory follows. There are some very good explanations covering our subject on the internet which we would like the user to read. One chapter has links to security guides and handbooks for Cisco routers which are marked as “must readings” because the users will work with those routers.

There is a second chapter in the external theory which holds a collection of interesting and recommended links to resources that could be useful to understand the goals of this module.

Before the participants do the pratical work, they are lead to a little chapter to test their knowledge. That should help them to see if they have understood the theory and if they are ready to go to the laboratory.

The hands-on section is the core if the “IP Security” module. It is the part where the students have to apply what they have learned so far. The first task is to configure the routers appropriately in such a way that the laboratory network is fully functional. The topology looks like follows:

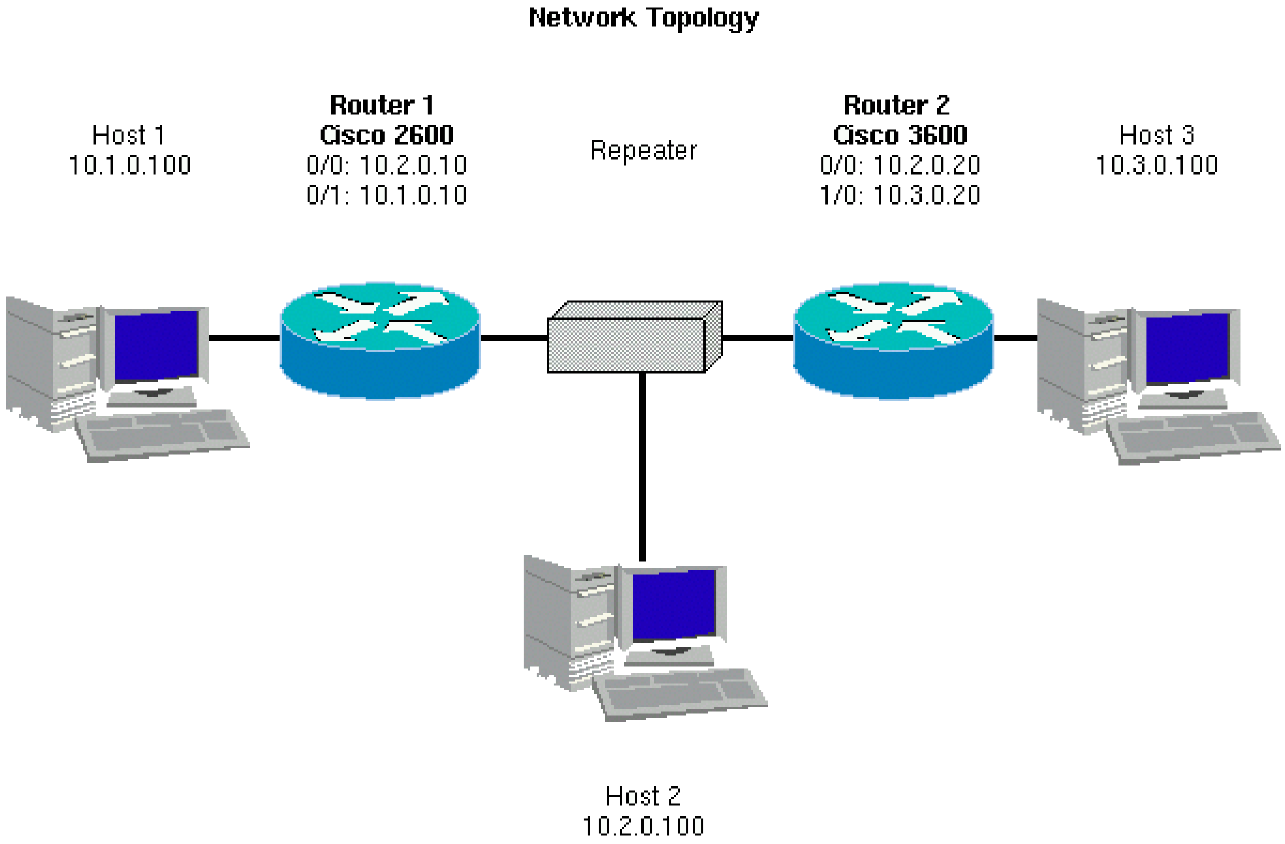


Figure 1: laboratory network topology

After they have configured the routers some network measurement tests have to be made as well as sniffing a telnet password to show that the data is indeed unencripted so far. The next task is to establish a IPSec VPN between two subnets on the routers. Finally the same tests have to be made that have been done before the VPN. This time the network throughput should be significantly lower and they should not be able to sniff the telnet password anymore.

The last task is to complete the “Post Laboratory Exercise”. This is a collection of question about what was being done during the hands-on part as well as some feedback questions.

4 IP Security Module Content

4.1 Introduction

First of all, welcome to the VITELS IP Security module.

In the introduction section we will inform you about everything you have to know and also about the goals of your work.

The module IP Security was created by the group ”Rechnernetze und verteilte Systeme” (RVS) of the ”Institute of Informatics and Applied Mathematics” (IAM) at ”University of Bern” (Unibe).

Click on Video in the active menu bar to see an introduction of the head of the RVS group, Prof. Dr. T. Braun.

For further information please feel free to email your comments to: steine@iam.unibe.ch .

Let’s go and work on real network equipment, no simplified simulations expect you here!

4.1.1 Tips and Tricks (Good to Know)

On this page you encounter important information about the working procedures for the module Internet Protocol Security (IP Security).

Many things you have learned in your compulsory lectures before are absolutely necessary for an understanding the following materia.

The module IP Security will introduce the basic elements of IPsec and give you the possibility to work on real Cisco routers for establishing an IPsec tunnel..

You should agree with all the points below...

- It is highly recommeded that you have worked through and have understood the entire preceeding modules .
- Be sure to understand the theoretical stuff before proceding to the laboratory section (and don’t forget to book the lab).
- The time you can spend in the laboratory itself is limited to 3 hours and you will not be able to do the theoretical and practical work at the same time.
- Use the ”Self Test” where it is available, follow the links in case of wrong answers.
- Quizzes are mandatory and are reviewed by a tutor.

... before going on to the next pages!

4.1.2 Goals

There are a many things you should have understood after absolving this course module. The major golas are listed below and should show you the minimal knowledge you must aquire.

- You understand the basic security concepts of the Internet, especially IPsec.
- You know how to ping and trace IP numbers in IP networks.
- You know how to make use of Tcpdump and understand the network dumps.
- You know how to perform bandwidth measurements in IP networks.
- You know how to configure IPsec tunnels on Cisco routers.

4.2 Theoretical Basics

In this section you get introduced into the theoretical basics of IP Security. Read carefully through the provided documents and take the time for understanding what you are reading.

After the theory section there is a readings section where you find more compulsory and recommended readings that can be selected using the Self-Test on the Knowledge page.

Learning in groups is certainly an advantage in many cases, although it cannot replace the monotone study phase where you have to get into a new area. But it definitely helps to overcome context problems in a later phase. WebCT addresses this issue by offering chat rooms, discussion boards and whiteboards. All these tools are open to you and should provide assistance.

4.2.1 Introduction

A Virtual Private Network (VPN) is a private network constructed by public lines or connections using secure methods to transfer information. For example, VPN technology allows organizations to securely extend their network services across shared public networks like the Internet to remote users, branch offices, and partner companies.

Large corporations used to interconnect local headquarters and branch offices with leased connections provided by telecommunication companies and ran private networks, so called corporate networks. With the rise of the Internet technology more and more corporate networks switched from various networking protocols such as Novell to the TCP/IP protocol suite. Such private networks based on Internet technology are also referred to as Intranets.

Since leased lines are expensive and the corporations often already have Internet connectivity, there is an economic incentive to replace the expensive leased connections and to use the wide area interconnectivity of the global Internet instead. However, there are two basic problems that must be emphasized:

- The Intranet may use private addresses that are not unique in the global Internet and thus not routable [RMK+96].
- The Internet protocol version 4 (RFC 791) does not assure transmission privacy. While IP packets travel through the public Internet they may be viewed or even altered by third parties.

4.2.2 Different Types of VPNs

There are many different types of Virtual Private Networks, they differ from protocols, abstractation layer, access types and so on. The next two subchapters will give you a brief overview of the various VPN types.

4.2.2.1 Subnet-To-Subnet and Access VPNs

Virtual private networks [FH98a, FH98b, and GHAM00] encapsulate the packets with private addresses into packets with public addresses. This process is called tunneling. If privacy and authenticity of the encapsulated packets is desired then this can be ensured with cryptographic means. Figure 2-1 shows the two most prominent VPN types: subnet-to-subnet VPNs and access VPNs. The subnet-to-subnet VPN interconnects geographically distributed private IP subnets. All traffic leaving one subnet destined for another one is tunneled through the public Internet. The access VPN allows roaming users to dial into the virtual network from their home computers or via an arbitrary Internet Point of Presence (POP). Figure 2-1 also illustrates the tunneling mechanism. It shows the structure of a tunneled IP packet originating from an application that runs within the private subnet X. The packet's destination is a computer in a remotely located part of the VPN (the private subnet Y). The subnets X and Y use private IP addresses that can not be routed in the public Internet. The address structure of the VPN is invisible from the outside. The access routers of subnets X and Y incorporate VPN functionality. They have an interior network interface with a private IP address and an exterior network interface with a public IP address. The access router at X recognizes that the packet in question must be tunneled. It knows the public interface of the access router of subnet Y and uses that address as destination address and its own public address as source address. The access router (also referred to as tunnel endpoint) creates a new IP packet with these new addresses and puts the original packet into the payload of the new packet. The payload is then encrypted. The new packet is sent to the tunnel endpoint at Y. There, the router extracts the payload of the packet and decrypts the content. Like this the original packet is restored and can be routed on the private subnet Y towards the originally intended destination. The access VPN case also uses tunnels. However, there are two distinct possibilities. Either the home PC acts as a tunnel endpoint or the POP of an Internet Service Provider (ISP) acts as tunnel endpoint. While a VPN may be useful for a small-to-medium sized company, the management of the VPN would require additional equipment and personnel. As a consequence, there exists a market for VPN services that lets the customers outsource the management of their VPN. The ISP can deploy VPN capable border routers and use them to introduce a VPN on-demand service [KBG00]. Thereby, several VPNs can be managed on the same infrastructure by the same personnel (ISP staff) so that both the customer and the provider can profit from the economy of scale.

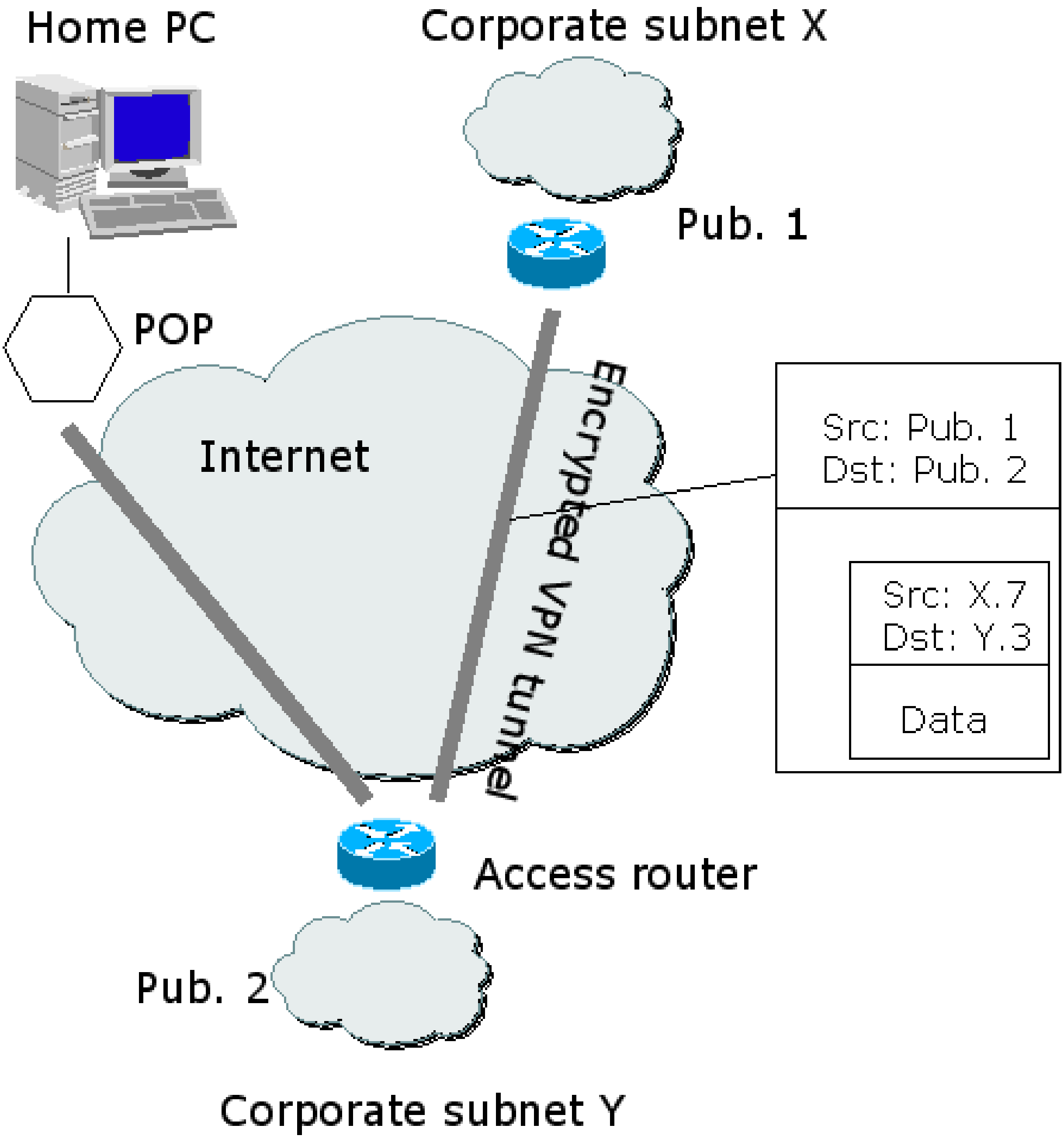


Figure 2: Virtual private network types

4.2.2.2 Encapsulation

Today, many different types of VPN technologies exist such as layer 2 VPNs based on Frame Relay and Asynchronous Transfer Mode (ATM) networks, remote access VPNs like PPTP and L2TP, and IPSec based VPNs.

4.2.2.2.1 Link Layer VPNs (Layer 2)

Integrated Services Digital Network (ISDN), Frame Relay and Asynchronous Transfer Mode are connection oriented networks on link level (layer 2) that support the establishment of link layer VPNs. Nowadays, most link layer VPNs are established by Frame Relay and ATM technology. IP network links over these underlying connection oriented network technologies are based on overlay models. In this case, meshes of connections have been established to interconnect IP routers of particular VPNs by providing a tunneling infrastructure. Another but similar types of virtual networks based on link level mechanisms are Virtual Local Area Networks (VLANs) that can be established using IEEE 802.1Q, ATM LAN Emulation (LANE) or Multi-Protocol Over ATM (MPOA). A major disadvantage of layer 2 VPNs and also VLANs is the need for a homogeneous topology throughout the entire VPN and the complexity to manage two different network technologies, i.e. IP and the underlying network technology, for a single VPN. An advantage lies in the connection oriented structure of those technologies. Links stay established and the tunneled packets follow the link and don't need to be routed as in IP based VPNs. In addition, Quality of Service (QoS) is often provided implicitly by the connection-oriented network technologies.

4.2.2.2.2 Network Layer VPNs (Layer 3)

In contrast to the link layer VPNs, where the location independent IP provides layer 3 addresses and the location dependent addresses are provided by layer 2 technology, in network layer VPNs, IP provides the location independent as well as the location dependent addressing. A link layer VPN example: the location independent IP addresses can be chosen by the user and the fixed Medium Access Channel (MAC) addresses are delivered by the network interface. A network layer VPN example: the location dependent IP addresses are provided by the Intranet and the location independent IP addresses are provided by the VPN. VPNs based on tunneling mechanisms that use network layer protocols such as IP or MPLS as outer header are called network layer VPNs. Tunneling (also called packet encapsulation) is a method of wrapping a packet into a new one by prepending a new header. The whole original packet becomes the payload of the new one. At the tunnel endpoints (usually border routers) the header is added respectively removed and the result is then forwarded again. Tunneling is often used to transparently transport packets of one network protocol through a network running another protocol.

IP VPN tunneling mechanisms often encapsulate IP packets into IP packets. This tunneling method is called IP in IP encapsulation (IPIP). With IPIP encapsulation encryption can be applied to the inner packet by using IPSec protocols.

Generic Routing Encapsulation (GRE) is another popular tunneling method. GRE is a multiprotocol carrier protocol. With GRE a router at each VPN site encapsulates protocol-specific packets in an IP header, creating a virtual point-to-point link to routers at other ends of an IP cloud, where the IP header is stripped off. By connecting multiprotocol subnetworks in a single-protocol backbone environment, IP tunneling allows network expansion across a single-protocol backbone environment. GRE tunnels do not provide true confidentiality (no encryption functionality) but can carry encrypted traffic. It is possible to encapsulate almost every existing network protocol in GRE.

Protocols such as the Point to Point Tunneling Protocol (PPTP) and the Layer 2 Forwarding (L2F) are required for supporting remote VPN access by single end systems. The protocols establish virtual point to point links between an end system and a VPN server. The VPN server acts as an interface of a VPN for remote end systems. The protocols mentioned above can carry any other network protocol and are themselves encapsulated in IP. PPTP and L2F have been developed further resulting in a standard called Layer 2 Tunneling Protocol (L2TP).

Firewalls and VPNs: VPN tunnels are mainly initiated and terminated by specially equipped routers equipped with the respective hard- and software for establishing VPNs. If the organization at the endpoint of a tunnel needs additional security, the router can be replaced by a firewall router. It is also possible to establish VPNs through firewalls, i.e. to tunnel a VPN link through a firewall. In the case of opening a firewall for a VPN tunnel, the instance allowing access to systems behind their firewall has to make sure that the other side deploys at least the same security policy level. If a host establishes a single unprotected connection to the Internet, and is at the same time connected through a VPN to computers behind a firewall, hackers can break in quite easily. The following paragraph is optional for reading:

With Multiprotocol Label Switching (MPLS) routing is independent from the destination address in the encapsulated packet. This independence from the routing decision and the destination address is obtained by establishing a Label Switched Path (LSP) instead of establishing an IP tunnel between the two routers of a common VPN. MPLS allows setting up tunnels by appending a MPLS header in front of the IP header. This 32-bit MPLS header avoids the large overhead by another IP header as it is required with IP-in-IP tunneling. Multiple MPLS headers are possible, i.e. labels can be stacked onto each other. Label stacking supports hierarchical tunnels and is in particular being used when building MPLS-based VPNs. In a typical MPLS VPN scenario as shown in Figure 2-2, a packet is classified at an ingress router of an ISP based on the incoming port number as belonging to a particular VPN. The ingress router has learned via Boarder Gateway Protocol (BGP) to which VPN it belongs, to which egress router the packet must be sent, and via which egress interface the destination is reachable. The ingress router appends two labels to a packet belonging to a VPN: The inner label specifies the egress port at the ISPs egress router, i.e. the link towards the destination subnetwork of the VPN. The outer label is being used to forward the packet towards the egress router and can be learned by MPLS signaling protocols such as Constraint-based Routing (CR) using Label Distribution Protocol CR-LDP or Traffic Engineering Resource Reservation Setup Protocol (TE-RSVP). Both labels are popped by the egress router (edge router). Figure 2-2 shows an example VPN/MPLS scenario with a label switched path (LSP) set up between ingress and egress of an ISP. This LSP is set up along the path and carries the traffic between the VPN subnets. Note that MPLS makes the private VPN addresses of a customer transparent to the routers of the ISP and that MPLS does not provide security mechanisms like IPSec does.

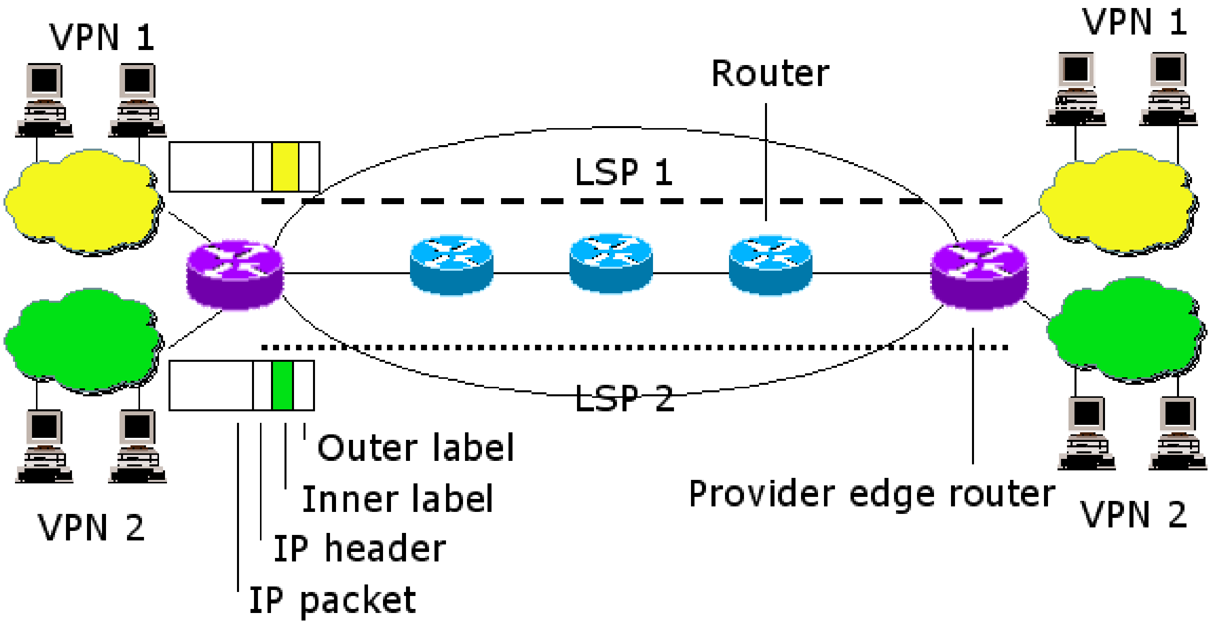


Figure 3: Different VPNs tunneled with MPLS over the same link

4.2.3 Security and the Internet Protocol

There exists a wide spectrum of technologies securing Internet communication but, most of them are dedicated to specific software applications. In that case, security is provided by the application layer. Good examples are Pretty Good Privacy (PGP) for mail encryption and browser-based authentication as well as Secure Sockets Layer (SSL) for traffic encryption between web browser and web server. These restrictions are not consistent with the requests of a large enterprise and the average ISP that may never know precisely the kind of applications running tomorrow over today's networks.

4.2.3.1 Possible Threats in the Internet

VPNs are driven by security threats in the network environment and must fulfill three fundamental requirements:

- Authentication: The communicating persons must really be the persons they claim to be.
- Confidentiality and privacy: No one shall be able to electronically eavesdrop traffic.
- Integrity: The received traffic must not be altered in any way during transmission.

4.2.3.1.1 Spoofing

In IP networks it is difficult to know where information really origins. An attack called IP spoofing takes advantage of this weakness. Since the source IP address of a packet has no influence on routing, it can easily be forged. In this type of attack, a packet coming from one machine appears as coming from another one. As a matter of fact, an IP source address is not trustable.

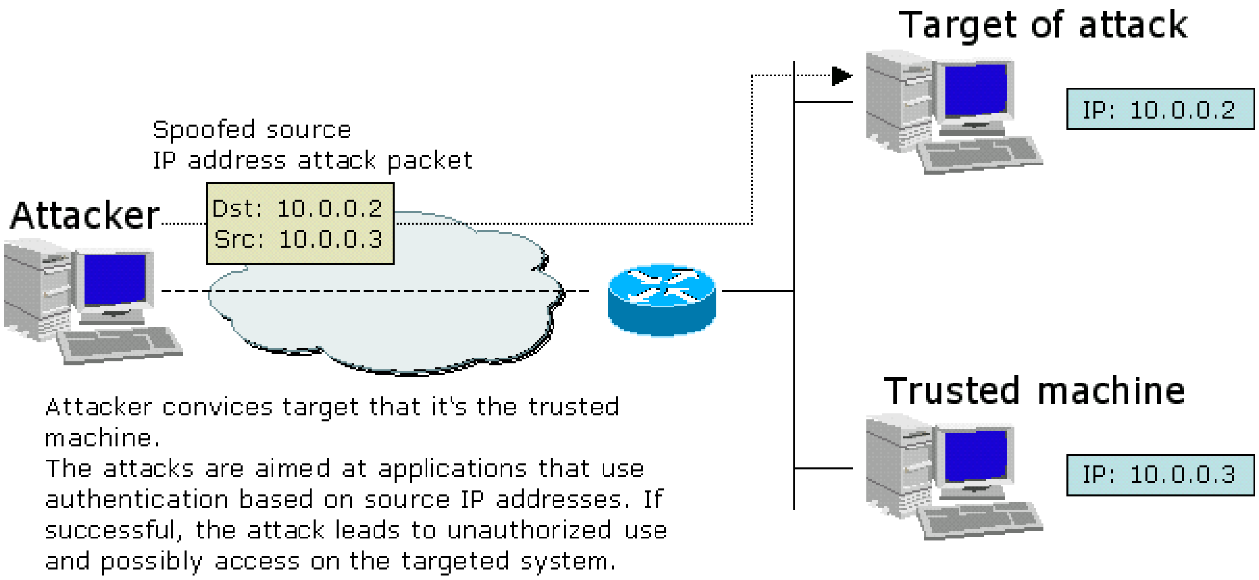
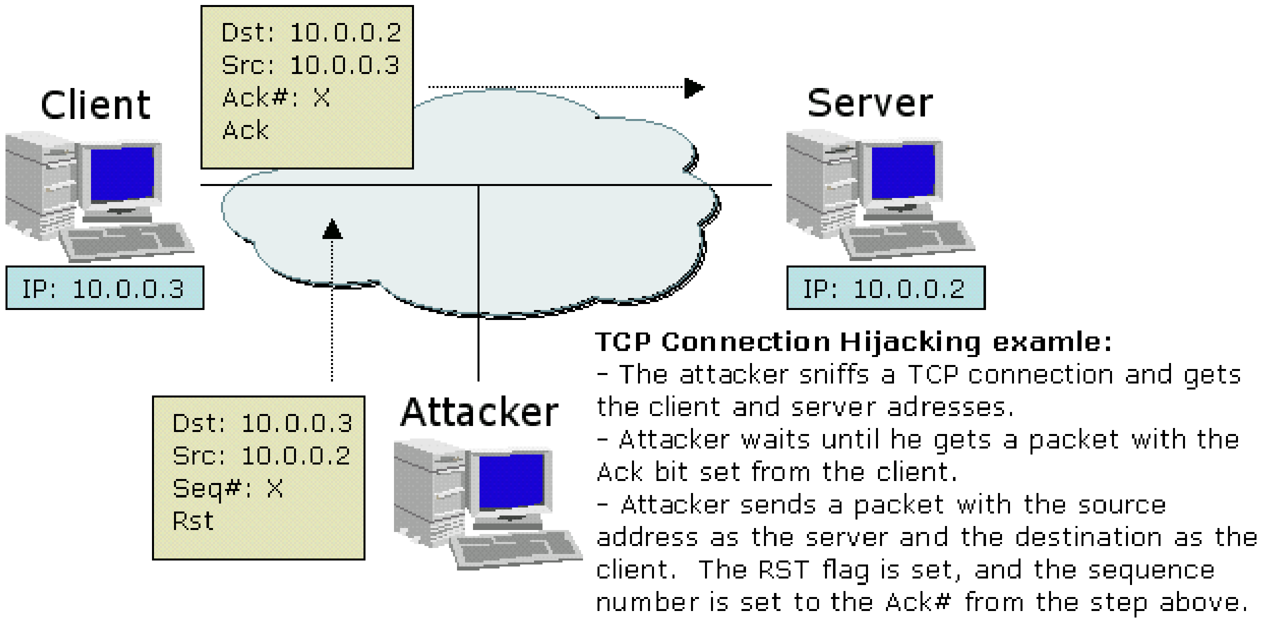

Target of attack
IP: 10.0.0.2
Spoofed source
IP address attack packet
Attacker
Dst: 10.0.0.2
Src: 10.0.0.3
Attacker convices target that it's the trusted machine.
The attacks are aimed at applications that use authentication based on source IP addresses. If successful, the attack leads to unauthorized use and possibly access on the targeted system.
Trusted machine
IP: 10.0.0.3

Figure 4: Demonstration of a source IP spoofing attack

4.2.3.1.2 Session Hijacking / Man in the Middle Attack

Spoofing makes it possible to take over a connection. Even initial authentication for each communication is no protection against session hijacking. A hacker can take over a session and stay invisible in the middle, pretending to be the respective peer of the two original session partners. He thereby possibly filters and modifies all packets of the session. Identifying the communicating person once does not ensure that it remains the same person throughout the rest of the session. Each data source has to be authenticated throughout the whole session.



TCP Connection Hijacking examle:
- The attacker sniffs a TCP connection and gets the client and server adresses.
- Attacker waits until he gets a packet with the Ack bit set from the client.
- Attacker sends a packet with the source address as the server and the destination as the client. The RST flag is set, and the sequence number is set to the Ack# from the step above.

Figure 5: TCP session hijacking example

4.2.3.1.3 Electronic Eavesdropping

A large part of most networks are based on Ethernet LANs. This technology has the advantage of being cheap, universally available, and easy to expand. But it has the disadvantage of making sniffing easy. An even more severe situation nowadays exists in wireless LANs. In Ethernet networks, every node can read each packet. Conventionally, each network interface card only listens and responds to packets specifically addressed to it. But it is easy to force these devices to collect every packet that passes on the wire. Physically, there is no way to detect from elsewhere on the network, which network interface card is working in the so-called promiscuous mode. Diagnostic tools called sniffers get the information out of the collected packets. Such tools can record all the network traffic and are normally be used to quickly determine what is happening on any segment of the network. However, in the hands of someone who wants to listen on sensitive communications, a sniffer is a powerful eavesdropping tool. The grown Internet structure with the global backbones makes electronic eavesdropping on routers and especially on backbone routers very efficient. Also in Virtual LANs that transfer clear text, packets can be eavesdropped easily.

4.2.3.2 The Security Architecture for the Internet Protocol (IPSec)

The Internet Engineering Task Force (IETF) standardized IP version 6 (IPv6) [DH98] to solve pending problems such as address shortage of the current version of the IP protocol (IPv4). A spin-off development of this process was the IP security architecture (IPSec) which introduces per-packet security features. While the IP version 6 deployment has been delayed, the security architecture has been adopted by the current IP version (IPv4). A key motivation for this was that IPSec includes all security mechanisms needed to implement VPNs. The Internet security architecture comprises of a family of protocols. IPSec describes IP packet header extensions and packet trailers that provide security functions. The per-packet security functions come from two protocols: The Authentication Header (AH) [KA98a] that provides packet integrity and authenticity and the Encapsulating Security Payload (ESP) [KA98b] that provides privacy through encryption. AH and ESP (Figures 3-1, 3-2 and 3-3) are independent protocols that can be used separately and that can be combined. One reason for the separation was that there are countries that have restrictive regulations on encrypted communication. There, IPSec can be deployed solely using AH because authentication mechanisms are not regulated.

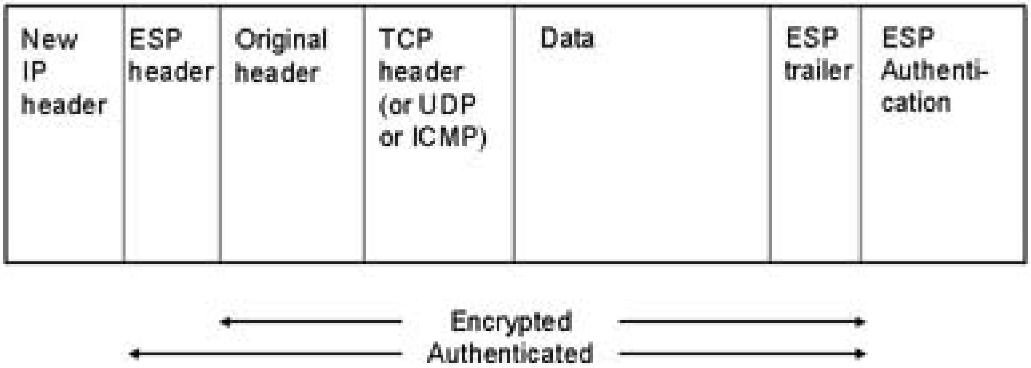


Figure 6: IPSec, IP packet after applying ESP in tunnel mode

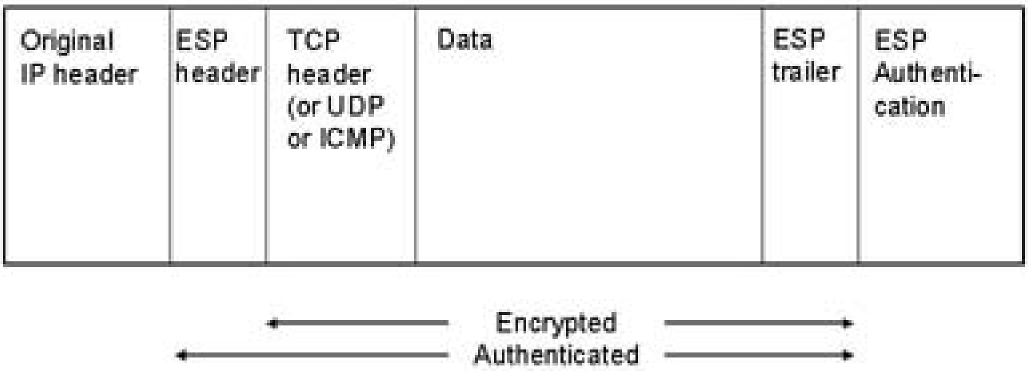


Figure 7: IPSec, IP packet after applying ESP in transport mode

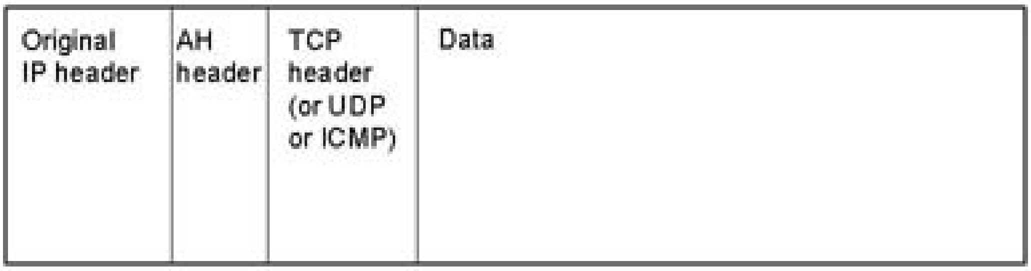


Figure 8: IPSec, IP packet after applying AH in transport mode

The set of AH and ESP is required in order to guarantee interoperability between different IPSec implementations. Both protocols are specified independently of cryptographic algorithms. A new encryption algorithm for example can easily be added to IPSec. Both AH and ESP assume the presence of a secret key. This key material may be installed manually. A better and more scalable approach is to use the third protocol of the IPSec family: the Internet Key Exchange protocol (IKE) [HC98] described below.

4.2.3.2.1 The Encapsulation Security Payload

The Internet Assigned Numbers Authority (IANA) has assigned the protocol number 50 for the IPSec encapsulation security payload. ESP ensures privacy of the IP payload. For that purpose an ESP header and an ESP trailer clamp the IP payload between them. The payload and the trailer are encrypted. The ESP also provides optional authentication. Figure 3-4 depicts the ESP part of an IP packet transformed by ESP in transport mode. The ESP header is located after the IP header and contains the security parameter index to identify the security association. Furthermore, there is a sequence number that is incremented for each packet. This helps to detect replay attacks, where the attacker records a packet and resends it later. The ESP trailer is added after the payload. The trailer includes padding that is necessary because the encryption algorithms often require the payload to be blocks of fixed length (e.g. 8 bytes). The pad length field encodes the length of the padding in bits. The next header field contains the protocol number of the next (eventually higher layer) protocol in the payload (e.g. IP or a concatenated IPSec protocol). Note that the trailer up to here is also encrypted. So, an attacker can for example not read what protocol is in the payload data. The ESP trailer may end with optional authentication data. The authentication data is a message authentication code (MAC) computed by a secure hash function. The input of the hash is a secret key, the ESP header, the ESP payload, and the rest of the ESP trailer. The MAC does not protect the initial IP header.

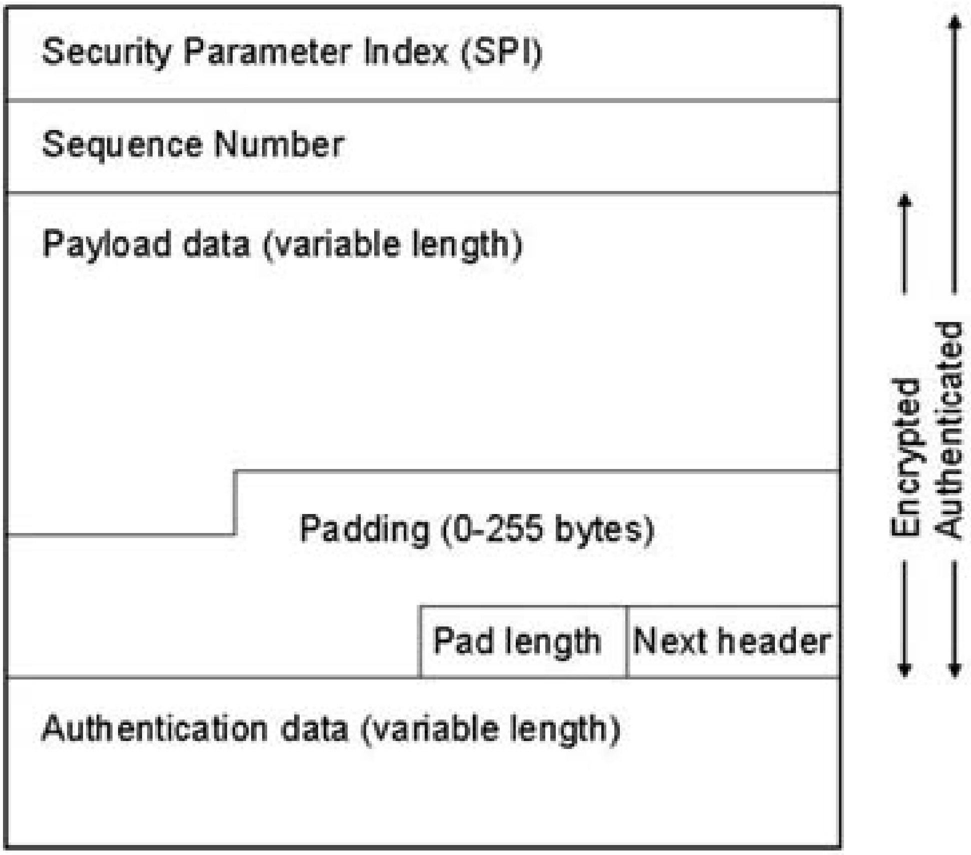
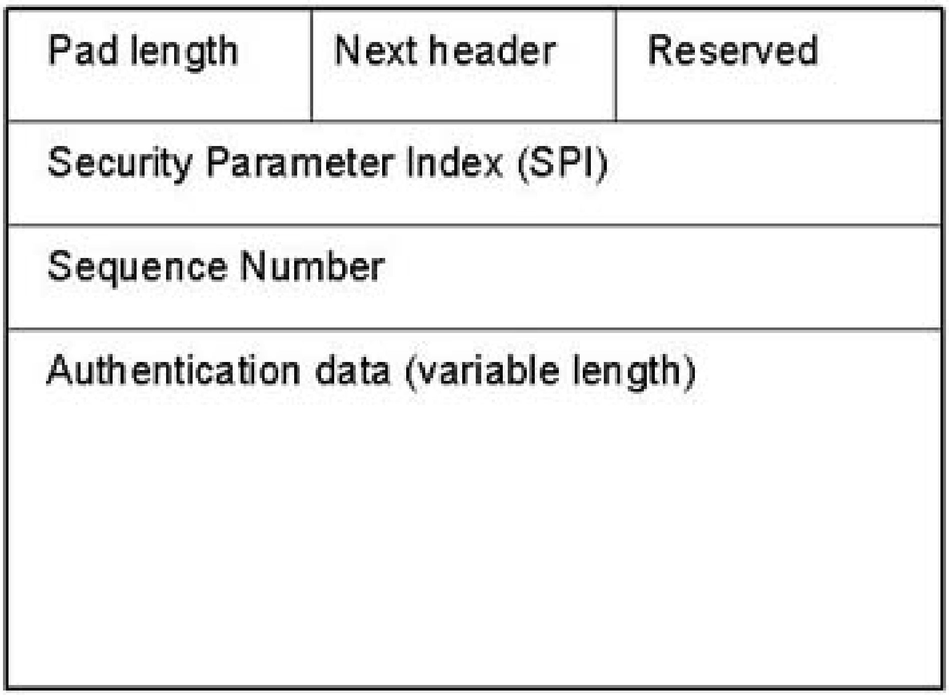

Security Parameter Index (SPI)
Sequence Number
Payload data (variable length)
Padding (0-255 bytes)
Pad length
Next header
Authentication data (variable length)
Encrypted
Authenticated

Figure 9: ESP part of an IPSec packet in transport mode

ESP supports nearly any kind of symmetric encryption. The default standard built into ESP, which assures basic interoperability, is 56-bit DES. ESP also supports some authentication (as AH does - the two options have been designed with some overlap).

4.2.3.2.2 The Authentication Header

The IANA has assigned the protocol number 51 for the IPSec authentication header. AH authenticates the packet so that a receiving IPSec peer can know for sure that the packet originates from the sending peer. Furthermore, the packet integrity is guaranteed. The receiver can verify that nobody has changed the packet while it was in transit between the peers. AH ensures this by calculating authentication data with a secure one-way hash function. The calculation also includes the secret key. An attacker not knowing this key is neither able to forge a valid packet nor to authenticate the packet. Figure 3-5 depicts the AH part of an IP packet transformed by AH in transport mode. The AH header includes the next header field and encodes the payload length. The length is necessary because the authentication data is variable in length. The AH header, just like the ESP header, contains a security parameter index and a sequence number. Finally, there is the authentication data (the secure hash value). The authentication of AH also covers the original IP header in contrast to the optional authentication of ESP. However, some fields of the IP header are excluded from the authentication, because their values may change during the forwarding of the packet. These exceptions are the time-to-live field that is decremented by each router and the Differentiated Services Code Point (DSCP).



Pad length	Next header	Reserved
Security Parameter Index (SPI)		
Sequence Number		
Authentication data (variable length)		

Figure 10: AH part of an IPSec packet

The design of the authentication header protocol makes it independent from the higher level protocol. It can be used with or without ESP. The different fields of the AH are:

- The next header field that specifies the higher level protocol following the AH.
- The Pad length field is an 8-bit value specifying the size of the AH.
- The reserved field is reserved for future use and is currently always set to zero.
- The SPI identifies a set of security parameters to be used for this connection.

- The sequence number is incremented for each packet sent with a given Security Parameter Index (SPI).
- Finally, the authentication data is the actual Integrity Check Value (ICV), or digital signature, for the packet. It may include padding to align the header length to an integral multiple of 32 bits (in IPv4) or 64 bits (in IPv6).

To guarantee minimal interoperability, all IPSec implementations must support at least HMAC-MD5 (Keyed-Hash Message Authentication Code for the Message Digest 5 Algorithm) and HMAC-SHA-1 (Keyed-Hash Message Authentication Code for Secure Hash 1 Algorithm) for AH. IPSec including AH and ESP has been designed for both IPv4 and IPv6.

4.2.3.3 Transport and Tunnel Mode

Both ESP and AH have two modes: the transport mode and the tunnel mode. Transport mode just encrypts and authenticates the payload and a part of the IP header. It extends the IP headers by adding new fields. Transport mode allows the user to run IPSec from end-to-end (Figure 3-6), while the tunnel mode is ideal for implementing a VPN tunnel at Internet access routers (Figure 3-7). The tunnel mode adds a complete new IP header (plus extension fields). In tunnel mode both AH and ESP can be used to implement IP-VPN tunnels. AH and ESP dispose of a small standardized set of cryptographic algorithms to ensure authenticity and privacy. Tunneling takes the original IP packet and encapsulates it within the ESP. Then it adds a new IP header to the packet containing the address of the IPSec gateways. This mode allows passing non-routable IP addresses or other protocols through a public network as the addresses of the inner header are hidden. Privacy is also given by hiding the original network topology.

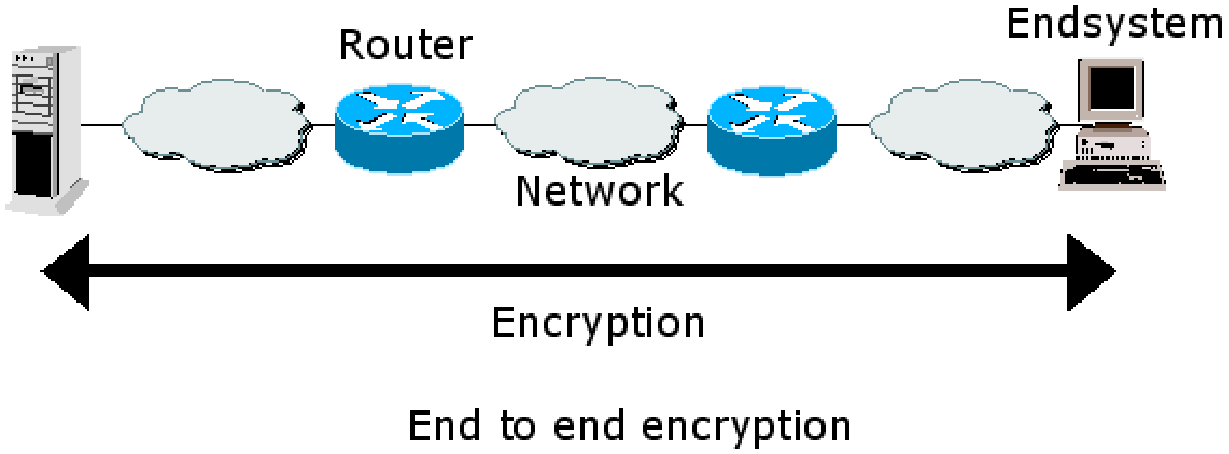


Figure 11: Transport mode

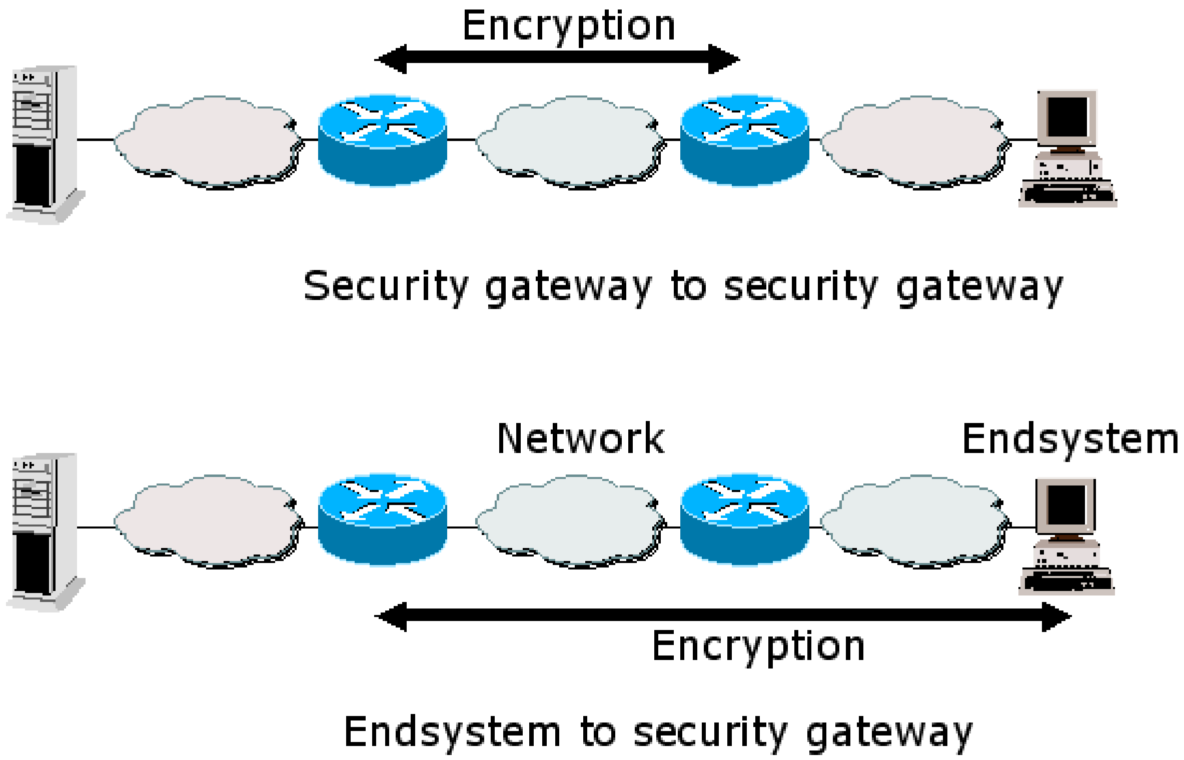

Encryption
Security gateway to security gateway
Network
Endsystem
Encryption
Endsystem to security gateway

Figure 12: Tunnel mode

4.2.3.4 Security Association and Security Policy Database

At some point in the network, both AH and ESP perform a transformation to IP packets. The IPSec compliant nodes always form sender-receiver pairs where the sender performs the transformation and the receiver reverses it. The relation between sender and receiver is described as a Security Association (SA). Note that the security association describes just one transformation and its inverse. Concatenated AH and ESP transformations are described by concatenated SAs. SAs can be seen as descriptions of ”open” IPSec connections. Both IPSec peering machines store representations of security associations. Under IPSec, the SA specifies the mode of the authentication algorithm used in the AH and the keys of that authentication algorithm. Also, it specifies the ESP encryption algorithm mode and the respective keys, the presence and size or absence of any cryptographic synchronization to be used in that encryption algorithm, how to authenticate traffic (protocols, encrypting algorithm and key), how to make communication private (again, algorithm and key), how often those keys need to be changed and the authentication algorithm, mode and transform for use in ESP plus the keys to be used by that algorithm. Finally it specifies the key lifetimes, the lifetime of the SA itself, the SA source address and a sensitivity level descriptor. A SA is uniquely identified by a triple consisting of a Security Parameter Index (SPI) (a 32-bit number), the destination IP address and the IPSec protocol (AH or ESP). The sending party writes the SPI into the appropriate field of the IP protocol extension. The receiver uses this information to identify the correct security association. In that way the receiver is able to invert the transformation and to restore the original packet. Each IPSec compliant machine may be involved in an arbitrary number of security associations. Accordingly, a SA is a management construct used to enforce a security policy in the IPSec environment. The policy specifications are stored locally in every IPSec node's Security Policy Database (SPD) that is consulted each time when processing inbound and outbound IP traffic, including non- IPSec traffic. The SPD contains different entries for inbound and outbound traffic. The SPD determines if traffic must be encrypted or can remain clear text or if traffic must be discarded. If traffic is encrypted, the SPD must point to the respective SA by a selector, a set of IP and upper layer protocol field values to map traffic to a policy.

4.2.3.5 The Internet Key Exchange Protocol

If two parties would like to communicate using authentication and encryption services they need to negotiate the protocols, encryption algorithms and keys to use. Afterwards they need to exchange keys (this might include changing them frequently) and keep track of all these agreements. The Internet Key Exchange protocol (IKE) allows two nodes to securely set up a security association by allowing these peers to negotiate the protocol (AH or ESP), the protocol mode, and the cryptographic algorithms to be used. Furthermore, IKE allows the peers to renew an established security association. IKE uses the Internet Security Association and Key Management Protocol (ISAKMP) [MSST98] to exchange messages. ISAKMP provides a framework for authentication and key exchange but does not define a particular key exchange scheme. IKE uses parts of the key exchange schemes Oakley [Orm98] and SKEME [Kra96]. IKE operates in two phases. In phase 1 the two peers establish a secure authenticated communication channel (also called ISAKMP security association). In phase 2 security associations can be established on behalf of other services (most prominently IPSec security associations). Phase 2 exchanges require an existing ISAKMP SA. Several phase 2 exchanges can be protected by one ISAKMP SA and a phase 2 exchange can negotiate several SAs on behalf of other services. ISAKMP SAs are bidirectional. The following attributes are used by IKE and are negotiated as part of the ISAKMP SA: encryption algorithm, hash algorithm, authentication method, and initial parameters for the Diffie-Hellman algorithm [Sch96]. Phase 1 exchange: IKE defines two modes for phase 1 exchanges: main mode and aggressive mode. The main mode consists of three request-response message pairs. The first two messages negotiate the policy (e.g. authentication method) (Figure 3-8a); the next two messages exchange Diffie-Hellman public values and ancillary data necessary for the key exchange (Figure 3-8b). The last two messages authenticate the Diffie-Hellman exchange (Figure 3-8c). The last two messages are encrypted and conceal the identity of the two peers.

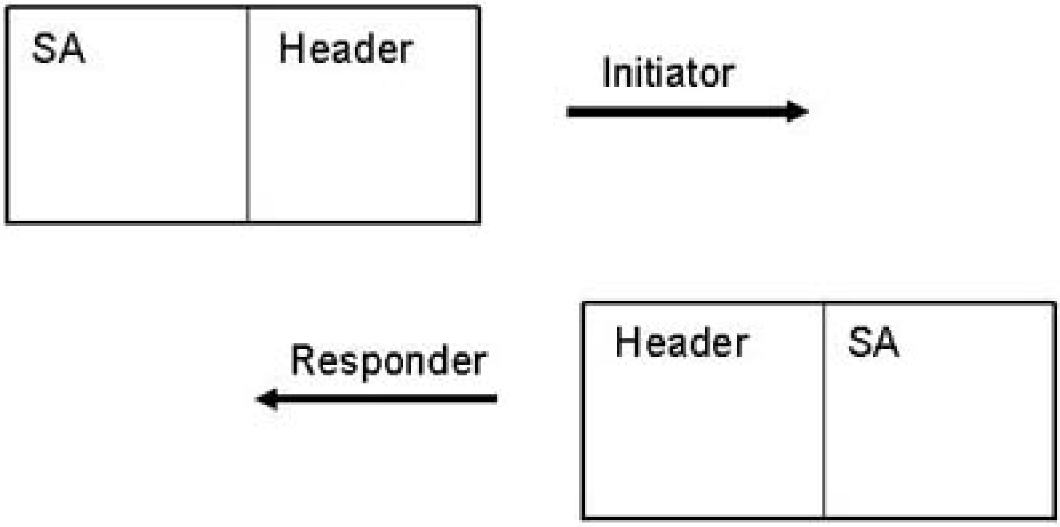


Figure 13: IKE main mode, first step

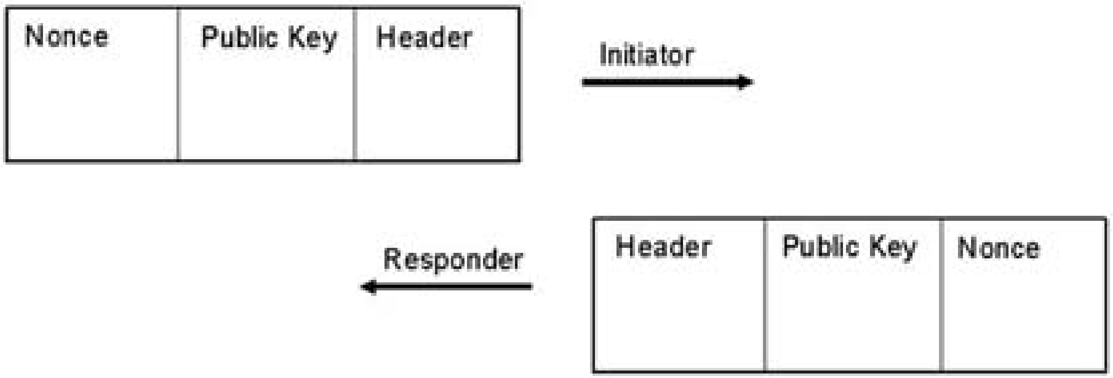


Figure 14: IKE main mode, second step

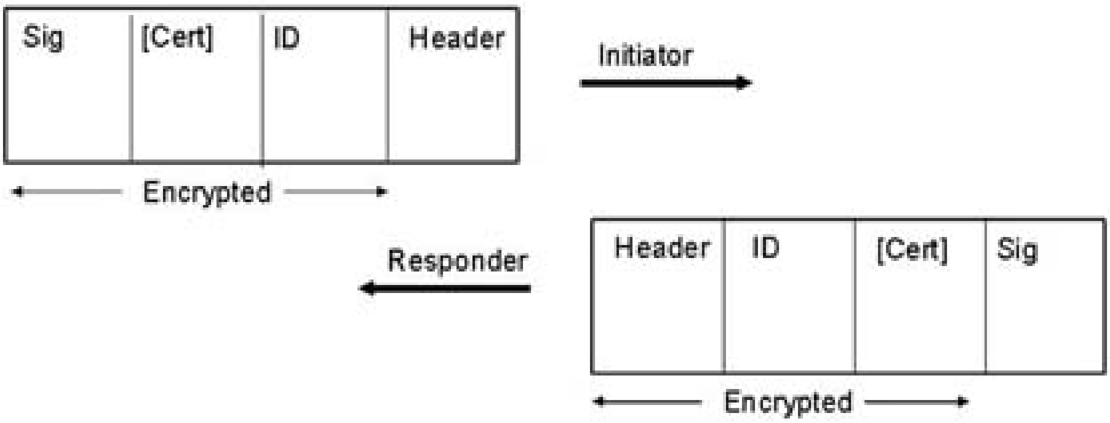


Figure 15: IKE main mode, third step

The aggressive mode of phase 1 consists of only three messages (Figure 3-9). The first message and its reply negotiate the policy. Moreover, they exchange Diffie-Hellman public values, ancillary data necessary for the key exchange as well as identities. In addition the second message authenticates the responder. The third message authenticates the initiator and provides a proof of participation in the exchange. The final message may be encrypted. Aggressive mode securely exchanges authenticated key material and sets up an ISAKMP SA, but it reveals the identities of the ISAKMP SA peers to eavesdroppers. Note, that the choice of the authentication method influences the specific composition of the payload of this exchange. Note also, that IKE assumes security policies that describe what options can be offered during the IKE negotiation.

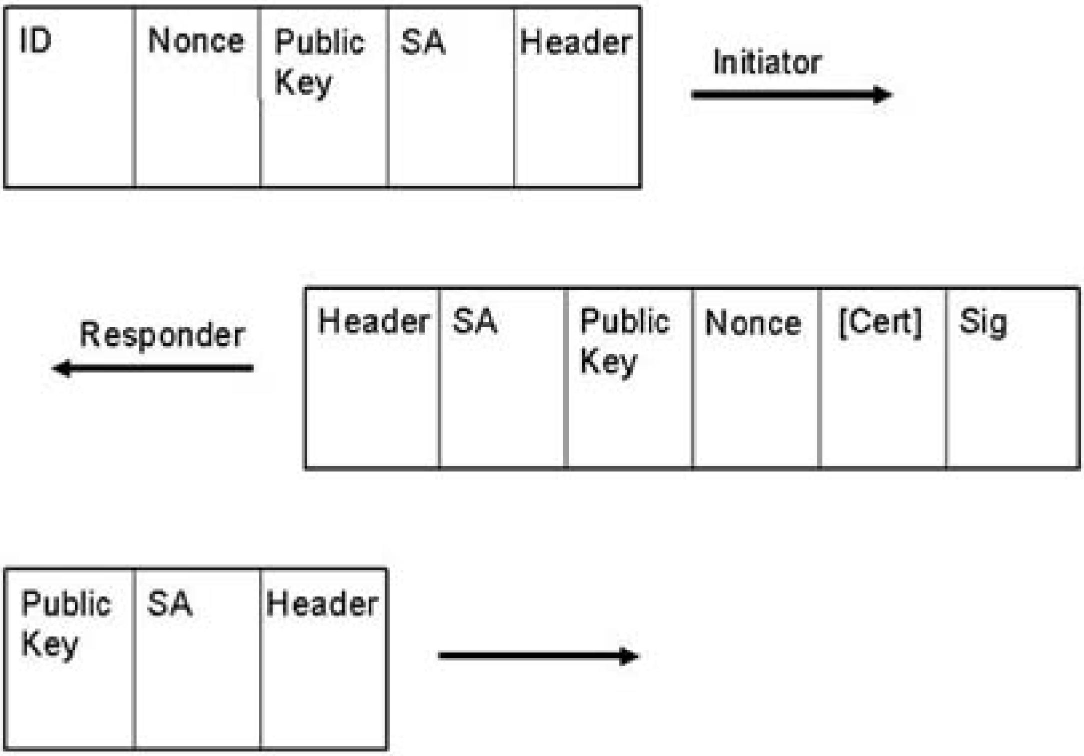


Figure 16: IKE aggressive mode

Phase 2 exchange: A phase 2 exchange negotiates security associations for other services and is protected (encrypted and authenticated) based on an existing ISAKMP security association. The payloads of all phase 2 messages are encrypted. A phase 2 exchange consists of three messages. The initiator sends a message containing a hash value, the proposed security association parameters and a nonce. The hash value is calculated over ISAKMP SA key material and proves authenticity. The nonce prevents replay attacks. Optionally, the initial message can also contain key exchange material. Such optional phase 2 key exchange generates key material which is independent from the key material of the ISAKMP SA. If the new SA should be broken, the ISAKMP SA is thus not compromised. The initial message may also contain identifiers in case the new SA is to be established between different peers than the ISAKMP SA peers. The responder replies with a message of the same structure as the initial message: an authenticating hash value, the selected SA parameters and a nonce. If the initial message contained optional parameters, then these are also part of the reply. Finally, the initiator acknowledges the exchange with a third and final message containing yet another hash value. Authentication: IKE establishes authenticated keying material. IKE supports four authentication methods to be used in phase 1: pre-shared secret keys, two forms of authentication with public key encryption, and digital signatures. Today's IKE implementations support X.509 certificates. Two computers not knowing each other can initialize a security association through the help of the commonly trusted third party that verified the certificates.

4.2.4 Outlook

The move from legacy technology based VPNs like Frame Relay and ATM to IP based VPNs will go on and thereby accelerate the deployment of newer VPN techniques like Generalized MPLS (G-MPLS). GMPLS is being considered as an extension to the MPLS framework to include optical, non-packet switched technologies. A recent traffic engineering technology development in the context of G-MPLS is Multiprotocol Lambda Switching (MP S). The major difference lies in the replacement of the traditional numeric MPLS labels by wavelengths (lambda). Another trend are mobile devices. Mobile users, as described above, move around and connect through fixed wire dial-up lines for example. These users are called nomadic users because the from the IP network view they remain locally immobile during a connection time. Roaming users that connect by mobile IP (MIP) require special solutions in the VPN area as with each handover of the mobile node the VPN tunnels need to be reestablished within very short time frames. An interesting combination of the IPSec suite and the MIP protocols is described in [DB01], where mobile hosts are allowed access to VPNs that are protected by firewalls from the public Internet.

4.2.5 Demonstration Applets

Here are some demonstration applets that may give you a visual explanation about some processes that have been mentioned in the theory.

- IPSec Packets (Applet) done by: Andreas Hosbach, Manuel Stadelmann & Thomas Staub
- Ip Routing (Applet) done by: Jol Marbach, Thomas Bernoulli, Christian Ammann & Marc Hugi
- Secret Key System (Applet) done by: MarcPhilippe Horvath, Adrian Kuhn & Maurice Seeberger
- MD5 Algorithm (Applet) done by: Oliver Aeberhard, Stefan Flury, Michael Mugglin & Daniel Kilchhofer
- Secure Sockets Layer and Transport Layer Security (Applet) done by: Beat Halter, David Joerg, Susanne Wenger & Vivian Kilchherr

All these applets were created by students of the University of Berne.

4.2.6 References

DB01 M. Danzeisen and T. Braun, Access of Mobile IP Users to Firewall Protected VPNs, Workshop on Wireless Local Networks at the 26th Annual IEEE Conference on Local Computer Networks (LCN'2001), Tampa, USA, Nov 15-16, 2001.

DH98 S. Deering and R. Hinden. Internet protocol, version 6 (IPv6) specification, December 1998. RFC 2460.

FH98a P. Ferguson and G. Huston. What is a VPN - part I. The Internet Protocol Journal, 1(1), 1998. [local copy]

FH98b P. Ferguson and G. Huston. What is a VPN - part II. The Internet Protocol Journal, 1(2), 1998. [local copy]

GHAM00 B. Gleeson, J. Heinanen, G. Armitage, and A. Malis. A framework for IP based virtual private networks, February 2000. RFC 2764.

HC98 D. Harkins and D. Carrel. The Internet Key Exchange (IKE), November 1998. RFC 2409.

GLHAM00 B. Gleeson, A. Lin, J. Heinanen, G. Armitage, A. Malis: A Framework for IP Based Virtual Private Networks, February 2000, RFC 2764.

KA98a S. Kent and R. Atkinson. IP authentication header, November 1998. RFC 2402.

KA98b S. Kent and R. Atkinson. IP encapsulating security payload (ESP), November 1998. RFC 2406.

KBG00 Ibrahim Khalil, Torsten Braun, and M. Gnter. Management of Quality of Service Enabled VPNs, IEEE Communications Magazine, May 2001. [local copy]

Kna96 Frederick Knabe. An overview of mobile agent programming. In Analysis and Verification of Multiple-Agent Languages, volume 1192 of Lecture Notes in Computer Science. Springer, June 1996. 5th LOMAPS Workshop. [local copy]

MSST98 D. Maughhan, M. Schertler, M. Schneider, and J. Turner. Internet security association and key management protocol, November 1998. RFC 2408.

Kra96 H. Krawczyk. SKEME: a versatile secure key exchange. In IEEE Proceedings of the Symposium on Network and distributed Systems Security, 1996. [local copy]

Orm98 H. Orman. The Oakley key determination protocol, November 1998. RFC 2412.

RMK+96 Y. Rekhter, B. Moskowitz, D. Karrenberg, G. J. de Groot, and E. Lear. Address allocation for private Internets, February 1996. RFC 1918.

Sch96 B. Schneier. Applied Cryptography. John Wiley and Son, 1996.

4.3 Readings

In this section you encounter a selection of readings grouped in must and recommended readings. The must readings are mandatory in contrast to the recommended readings that are a supplement for those that would like to know more ore have encountered problems in the self-test. In the recommended readings section you also find the references of the theory section.

Why do get so many readings and not only a small but necesary amount of readings? We want you to become used to what you are going to meet in your later career and therefore you should learn how to choose the best material.

4.3.1 Must Readings (check the knowledge section first)

- IPSec Network Security Guide for Cisco Routers
  http://www.cisco.com/univercd/cc/td/doc/product/software/ios113ed/113t/113t_3/ipsec.htm
- Configuring Network Data Encryption
  http://www.cisco.com/univercd/cc/td/doc/product/software/ios113ed/113ed_cr/secur_c/scprt4/scencryp.htm
- The Internet Protocol Journal - IP Security
  http://www.cisco.com/warp/public/759/ipj_3-1/ipj_3-1_ip.html

4.3.2 Recommended Readings (check the knowledge section first)

Books

- TCP/IP Network Administration, OReilly, 1998, Network Security, chapter 12
- VPN, OReilly, 1995, Basic VPN Technologies, chapter 2, Creating a VPN with the Unix Secure Shell, chapter 8, pages 11 - 42 and 135 - 160
- VPN, OReilly, 1995
- Building and Managing VPN, Dave Kosiur, Wiley, 1998

Cisco Router Specific Documents

- Cisco 2600/3600 Software Configuration Guide
  http://www.cisco.com/univercd/cc/td/doc/product/access/acs_mod/cis3700/sw_conf/37_swcf/index.htm
- Layer 2 Tunneling Protocol
  http://www.cisco.com/warp/public/cc/pd/iosw/prodlit/l2tun_ds.htm
- IPSec Network Security for Cisco Routers
  http://www.cisco.com/univercd/cc/td/doc/product/software/ios113ed/113t/113t_3/ipsec.htm

IPSec/VPN Related Articles

- IBM VPN Overview
  http://www-3.ibm.com/software/network/library/whitepapers/vpn/index.html
- FreeS/WAN IPSec Documentation
  http://www.freeswan.org/freeswan_trees/freeswan-1.95/doc/ipsec.html
- An IPSec Primer (Universit Libre de Bruxelles)
  http://www.iihe.ac.be/scimitar/J1000/ipsec

IPSec RFC's

- Security Architecture for the Internet Protocol (RFC 2401)
  http://www.ietf.org/rfc/rfc2401.txt
- IP Authentication Header (RFC 2402)
  http://www.ietf.org/rfc/rfc2402.txt
- IP Encapsulating Security Payload (ESP) (RFC 2406)
  http://www.ietf.org/rfc/rfc2406.txt

RMK+96 Address Allocation for Private Internets
http://www.ietf.org/rfc/rfc1918.txt

4.4 Test Your Knowledge

4.4.1 Self Test

Learn if you know the correct answers to the questions in "Self Test", located in the action menu. If you don't know abbreviations or are insecure answering a question, go to the indicated reading section and pick the corresponding reading to improve your knowledge. The self test is for your personal use, no teacher will ever see your answers and rate you.

4.4.2 Quiz

If you have updated your knowledge and feel ready for the practical session, solve the "Quiz" located in the action menu. Quiz results are reviewed by your tutor. You can start with the lab session even if the quiz hasn't been reviewed yet.

4.5 Laboratory Session

It was upon a time when computer network laboratories used to look like this:

And students had a hard life attending classes at university:

But fortunately network laboratories have evolved and students can stay at home when doing the practical work:

4.5.1 Where do you do what?

As already mentioned before, the practical session is timely limited. As a consequence, you are only allowed to proceed after successfully passing the knowledge quiz of chapter 4.

You can log-in to the practical part of the IP Security module only if you have reserved before. If you would like to book now: Scheduling. If you have booked before and already possess your time slot go on here: IP Security Lab Session.

During the practical work you will connect with secure shells to the specific machines. The shells are run from your computer as Java applets. You can open as many of them as you need (i.e. one per machine).

We will guide you through the module with the WebCT pages.

4.5.2 Practical Work

4.5.2.1 What are you going to do?

- You will learn how to configure Cisco routers and set-up routing with RIP,
- you will establish a VPN-tunnel betweeen two routers,
- you will perform pings,
- traceroutes,
- bandwith measurements,
- sniffing passwords,
- both before and after establishing the VPN tunnel.

4.5.2.2 What if you get lost?

At the page where you can login to the hosts and routers, there is an emergency button. Click this link and the routers will be set to 0!

4.5.2.3 An important note about the routers

Please do not set any passwords on the cisco routers! Please follow these instructions to reset the routers before you begin with the lab session (step by step):

log into to the routers and then type the following:

1. enable

2. erase startup-config
3. confirm with [return]
4. reload
5. System configuration has been modified. Save? [yes/no]: no
6. confirm with [return]
7. wait
8. Would you like to enter the initial configuration dialog? [yes/no]: no
9. press [return] for router-prompt

1. important note: after entering 'reload' you have to answer the following question with 'no': System configuration has been modified. Save? [yes/no]: no
2. after the reset, please answer the following question with 'no' as well (if you would answer with 'yes', you would be forced to enter a password): Would you like to enter the initial configuration dialog? [yes/no]: no

4.5.3 Step by Step

Let's go and work through the laboratory. There are four sections to pass. Copy and paste the screens from the shells when you are invited to do so. You need theses results later-on in the quiz.

4.5.4 Setting up RIP

Follow the task list below:

- Passwords: there are no passwords set on the routers. Please do not set any passwords on the cisco routers!
- Since you will configure the cisco routers via the terminal console, here are some tips using it:
  - use tab-completion
  - you can type a "?" at any time to get a list of available commands or parameters.
  - check your configuration with the "show" commands. For example "show ip interface brief" or "show ip route" after configuring the interfaces and the routing.
- First of all log into both Cisco routers and erase the current config. To do this follow the instruction on chapter 5.2.3 An important note about the routers.
- The next step is to give the routers a hostname and to configure their interfaces like in the image below. If you experience problems configuring the interfaces read the section "Configuring Ethernet Interfaces" and "Configuring Fast Ethernet Interfaces" of the "Software Configuration Guide for Cisco 3600 Series and Cisco 2600 Series Routers" which is linked at the 3.2 Recommended Readings page. (Hint: be sure to set up their interfaces as no shutdown.)
- After you have configured the interfaces set up the ip routing. Use RIP version 2 for routing. (Do you have problems with RIP? click here for more hints)

4.5.5 Testing RIP

Perform these tests to see if your network is running properly:

- Ping every host in your net, from host to host and from router to host. Retry but use the command ”debug ip packet” first.
- Use traceroute to examine your connections.
- Use netpipe (the command is: ”NPtcp”) to measure the bandwidth from Host 1 to Host 3. You also might want to specify a different increment set, check the NPTcp usage for parameters. Save the output for the post lab work.
- Make a telnet session between Host 1 and Host 3 and try to sniff the password using tcpdump on Host 2. Save the dump for post lab work and mark the sniffed password characters somehow. (Do you have problems with tcpdump? click here for more hints)

4.5.6 Setting up the VPN

Follow the task list below:

- Create DSS keys on the routers.
- Exchange the DSS keys.
- Configure the routers to encrypt both TCP and UDP traffic between the two subnet 10.1.0.0/24 and 10.3.0.0/24.
- Make sure the routers use des (Data Encryption Standard) algorithm with a Cipher Feedback Modus (CFB) of 64 bit.
- (Do you have problems with setting up a secure vpn? click here for more hints)

4.5.7 Test the VPN

Perform these tests to see if your network is running properly:

- Ping every host in your net, from host to host and from router to host. Retry but use the command ”debug ip packet” first.
- Use traceroute to examine your connections.
- Use netpipe to measure the bandwidth from Host 1 to Host 3, just like you did on chapter 5.5. Save the output for the post lab work.
- Make a telnet session between Host 1 and Host 3 and try to sniff the password using tcpdump on Host 2. Save the dump for post lab work and mark the encrypted password characters somehow. Verify if packet data is encrypted.

4.6 Post Laboratory Exercises

After the Lab session, you should be able to solve these exercises. Please verify that you have your output from the lab exercise handy when you start the post lab quiz.

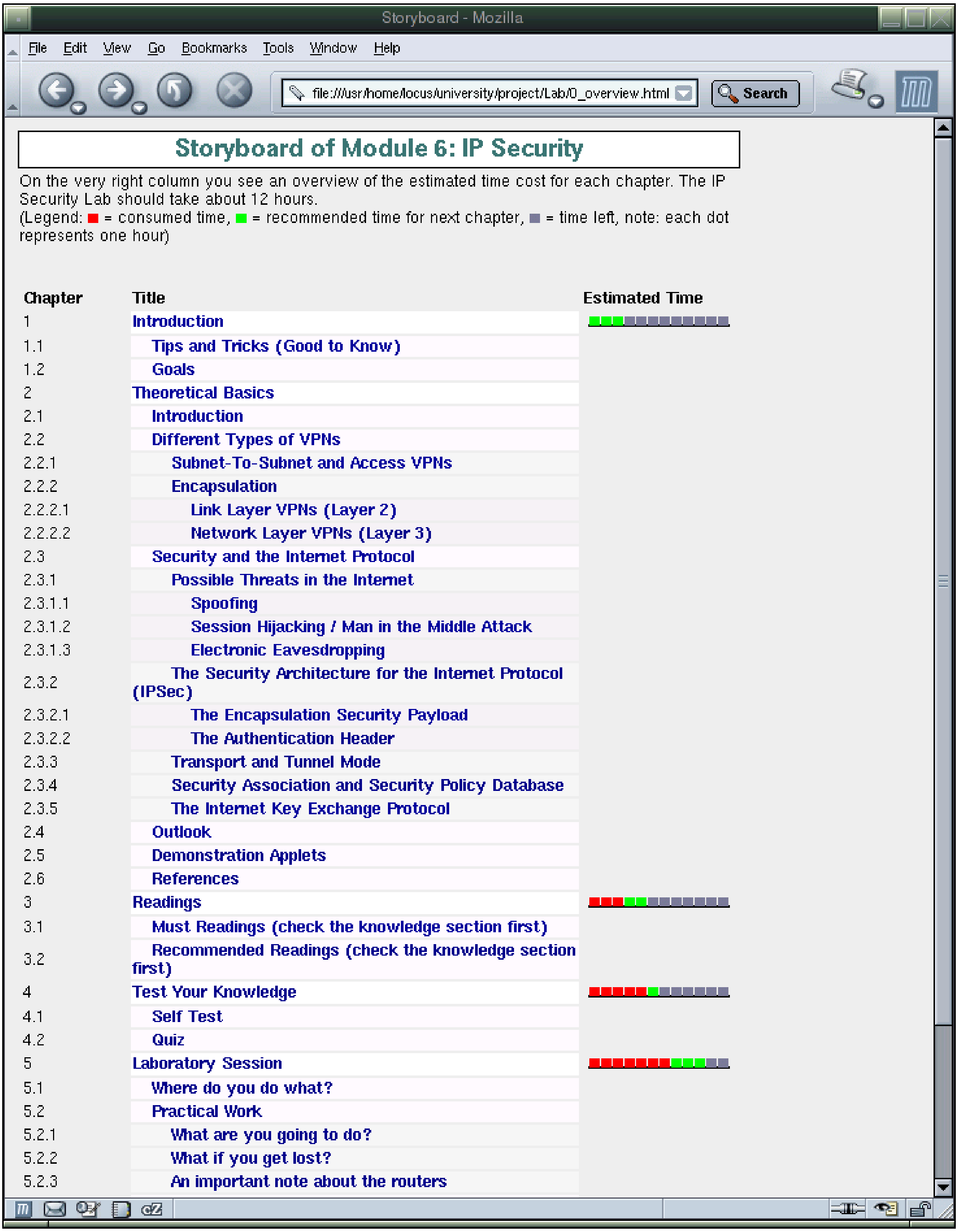
Click on ”Quiz” in the action menu.

4.7 Frequently Asked Questions

empty

5 Screenshots

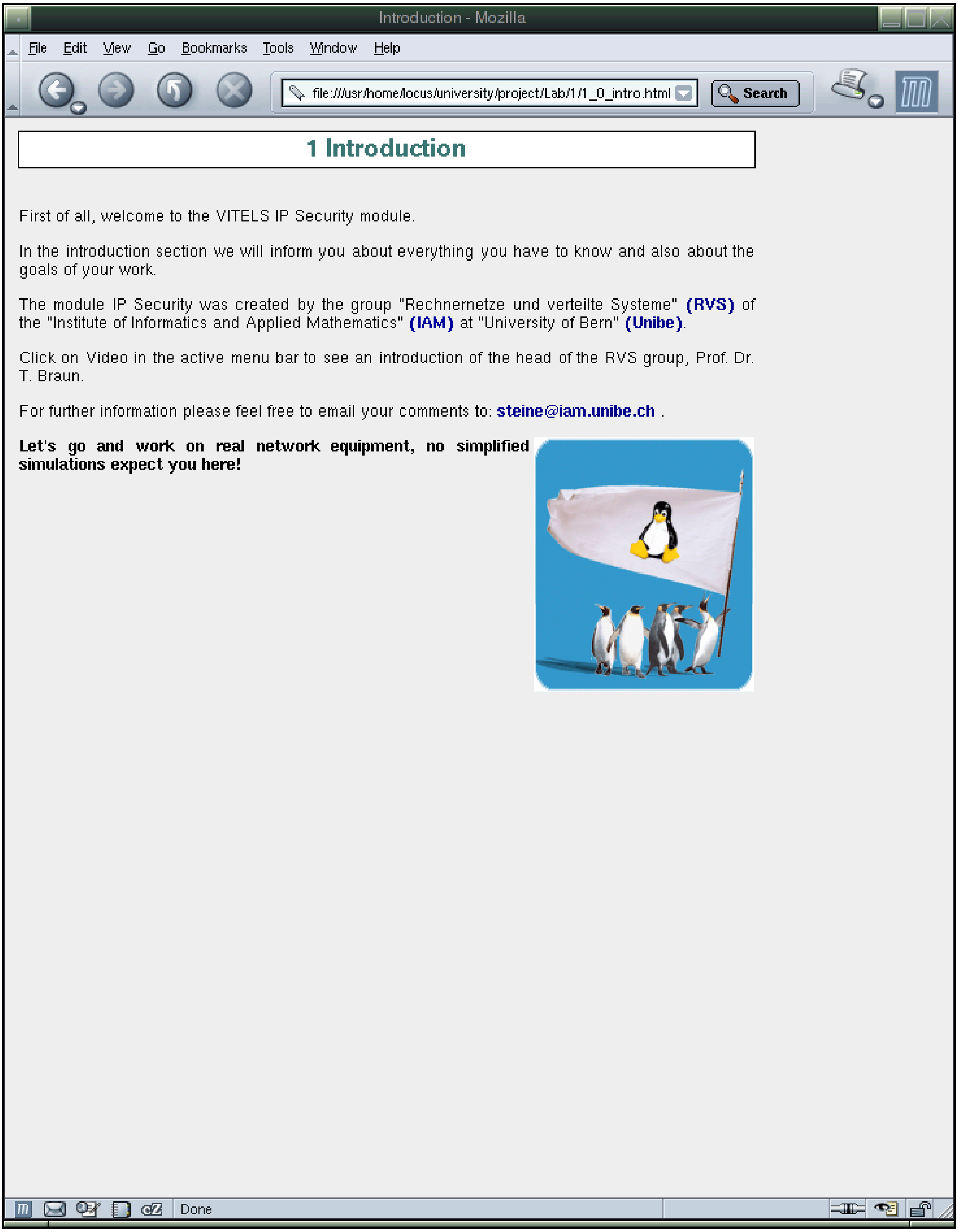
This section shows how the module “IP Security” actually looks like and how it was designed.


Storyboard - Mozilla
File Edit View Go Bookmarks Tools Window Help
file:///usr/home/locus/university/project/Lab/0_overview.html
Search

Storyboard of Module 6: IP Security

On the very right column you see an overview of the estimated time cost for each chapter. The IP Security Lab should take about 12 hours.
(Legend: 🟥 = consumed time, 🟩 = recommended time for next chapter, ⬛ = time left, note: each dot represents one hour)

Chapter	Title	Estimated Time
1	Introduction	🟩🟩🟩⬛⬛⬛⬛⬛⬛⬛⬛⬛
1.1	Tips and Tricks (Good to Know)	
1.2	Goals	
2	Theoretical Basics	
2.1	Introduction	
2.2	Different Types of VPNs	
2.2.1	Subnet-To-Subnet and Access VPNs	
2.2.2	Encapsulation	
2.2.2.1	Link Layer VPNs (Layer 2)	
2.2.2.2	Network Layer VPNs (Layer 3)	
2.3	Security and the Internet Protocol	
2.3.1	Possible Threats in the Internet	
2.3.1.1	Spoofing	
2.3.1.2	Session Hijacking / Man in the Middle Attack	
2.3.1.3	Electronic Eavesdropping	
2.3.2	The Security Architecture for the Internet Protocol (IPSec)	
2.3.2.1	The Encapsulation Security Payload	
2.3.2.2	The Authentication Header	
2.3.3	Transport and Tunnel Mode	
2.3.4	Security Association and Security Policy Database	
2.3.5	The Internet Key Exchange Protocol	
2.4	Outlook	
2.5	Demonstration Applets	
2.6	References	
3	Readings	🟥🟥🟥🟩🟩⬛⬛⬛⬛⬛⬛⬛
3.1	Must Readings (check the knowledge section first)	
3.2	Recommended Readings (check the knowledge section first)	
4	Test Your Knowledge	🟥🟥🟥🟥🟥🟩⬛⬛⬛⬛⬛⬛
4.1	Self Test	
4.2	Quiz	
5	Laboratory Session	🟥🟥🟥🟥🟥🟥🟥🟩🟩🟩⬛⬛
5.1	Where do you do what?	
5.2	Practical Work	
5.2.1	What are you going to do?	
5.2.2	What if you get lost?	
5.2.3	An important note about the routers	


Introduction - Mozilla
File Edit View Go Bookmarks Tools Window Help
file:///usr/home/locus/university/project/Lab/1/1_0_intro.html
Search
Done

1 Introduction

First of all, welcome to the VITELS IP Security module.

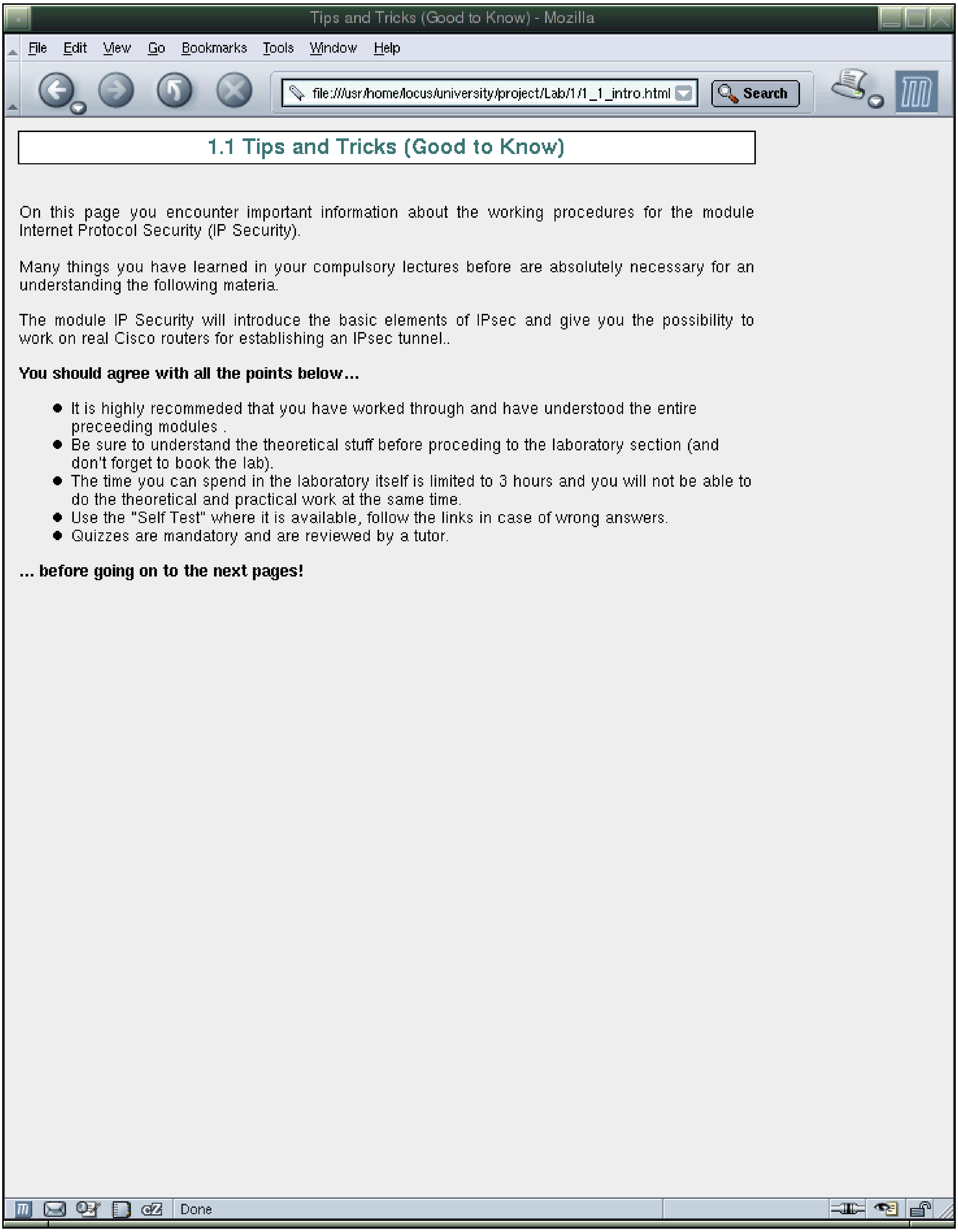
In the introduction section we will inform you about everything you have to know and also about the goals of your work.

The module IP Security was created by the group "Rechnernetze und verteilte Systeme" **(RVS)** of the "Institute of Informatics and Applied Mathematics" **(IAM)** at "University of Bern" **(Unibe)**.

Click on Video in the active menu bar to see an introduction of the head of the RVS group, Prof. Dr. T. Braun.

For further information please feel free to email your comments to: **steine@iam.unibe.ch** .

Let's go and work on real network equipment, no simplified simulations expect you here!


Tips and Tricks (Good to Know) - Mozilla
File Edit View Go Bookmarks Tools Window Help
file:///usr/home/locus/university/project/Lab/1/1_1_intro.html
Search
Done

1.1 Tips and Tricks (Good to Know)

On this page you encounter important information about the working procedures for the module Internet Protocol Security (IP Security).

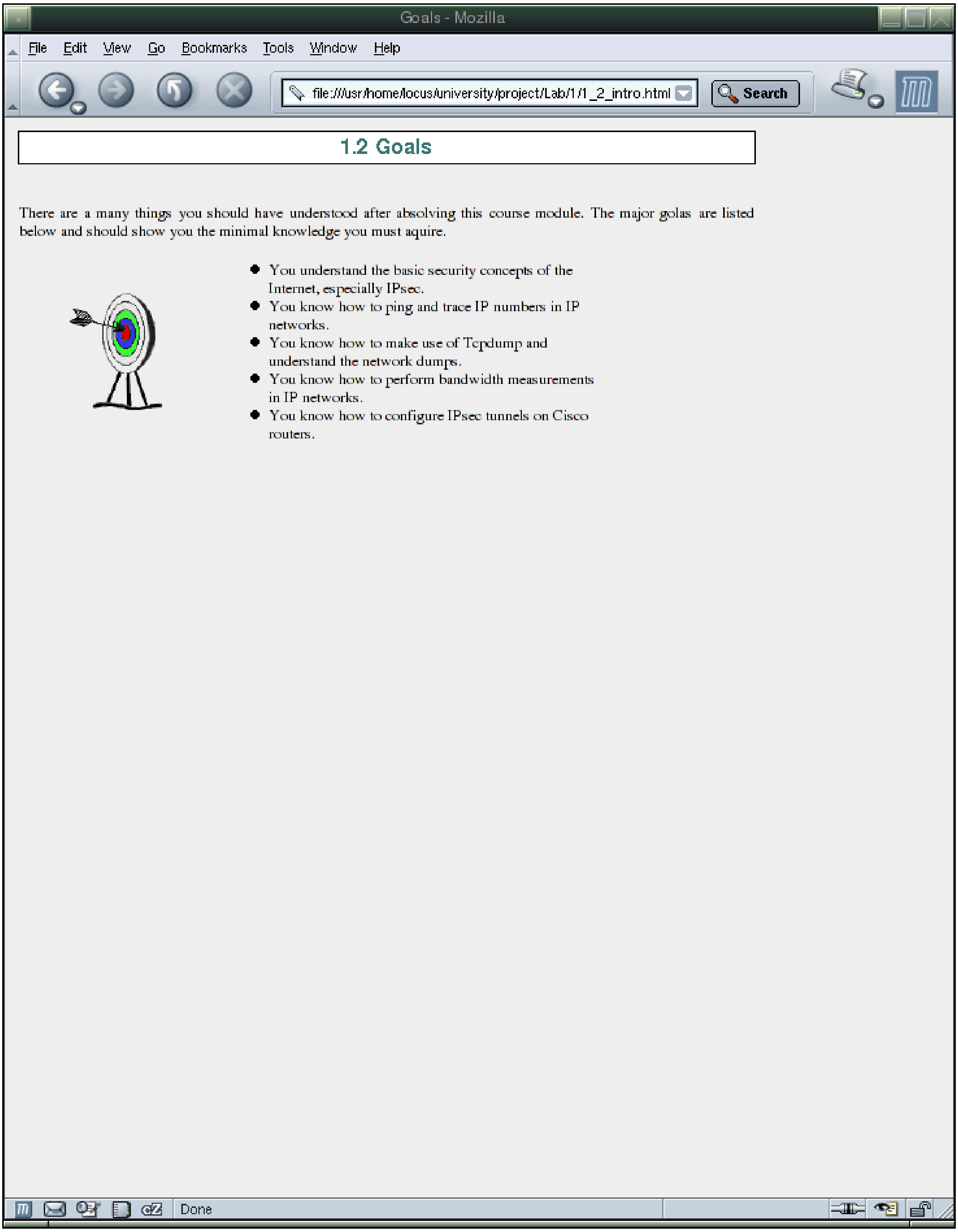
Many things you have learned in your compulsory lectures before are absolutely necessary for an understanding the following materia.

The module IP Security will introduce the basic elements of IPsec and give you the possibility to work on real Cisco routers for establishing an IPsec tunnel..

You should agree with all the points below...

- It is highly recommeded that you have worked through and have understood the entire preceeding modules .
- Be sure to understand the theoretical stuff before proceding to the laboratory section (and don't forget to book the lab).
- The time you can spend in the laboratory itself is limited to 3 hours and you will not be able to do the theoretical and practical work at the same time.
- Use the "Self Test" where it is available, follow the links in case of wrong answers.
- Quizzes are mandatory and are reviewed by a tutor.

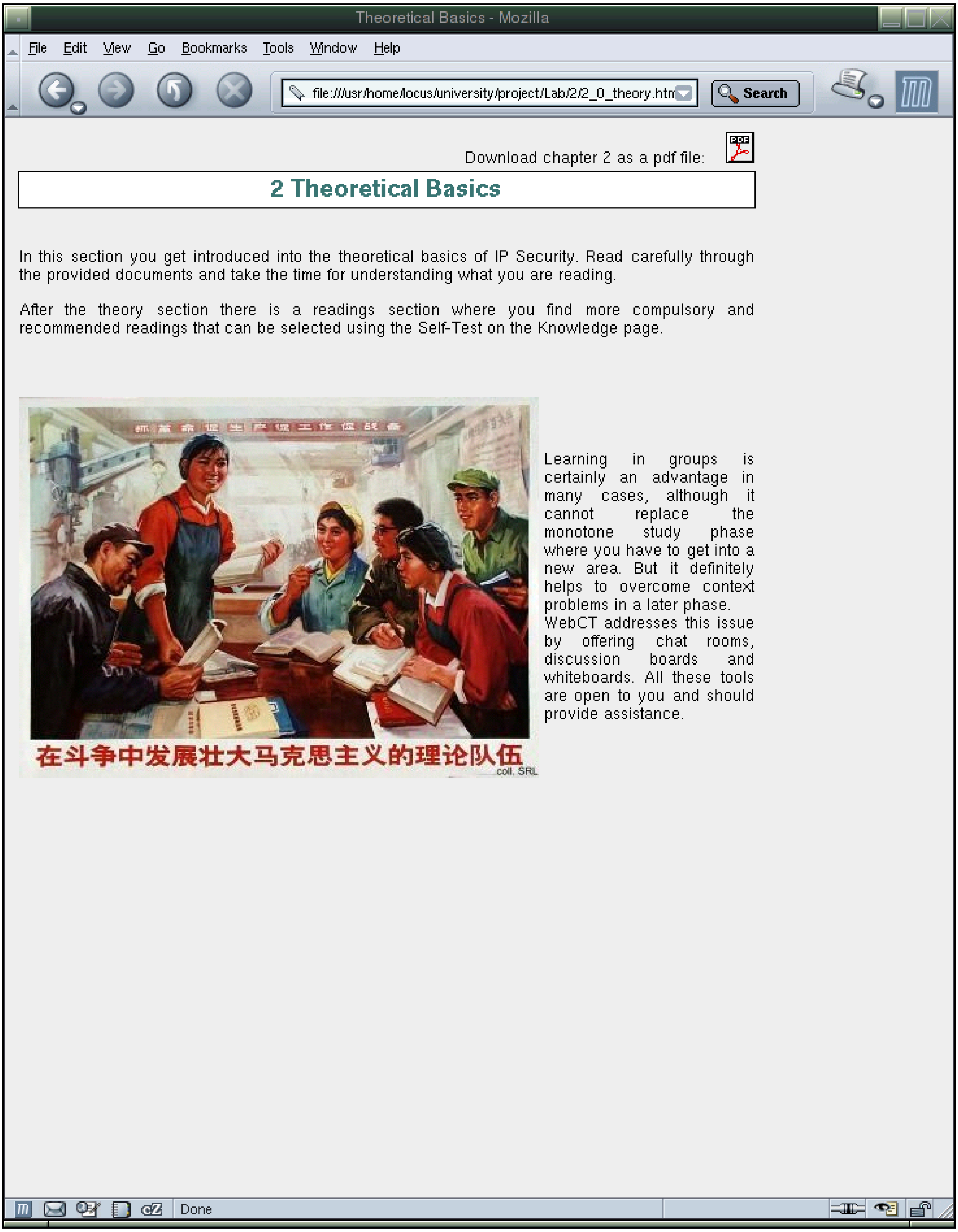
... before going on to the next pages!



1.2 Goals

There are a many things you should have understood after absolving this course module. The major golas are listed below and should show you the minimal knowledge you must aquire.

- You understand the basic security concepts of the Internet, especially IPsec.
- You know how to ping and trace IP numbers in IP networks.
- You know how to make use of Tcpdump and understand the network dumps.
- You know how to perform bandwidth measurements in IP networks.
- You know how to configure IPsec tunnels on Cisco routers.


Theoretical Basics - Mozilla
File
Edit
View
Go
Bookmarks
Tools
Window
Help
file:///usr/home/locus/university/project/Lab/2/2_0_theory.htm
Search
在斗争中发展壮大马克思主义的理论队伍
coll. SRL
Done

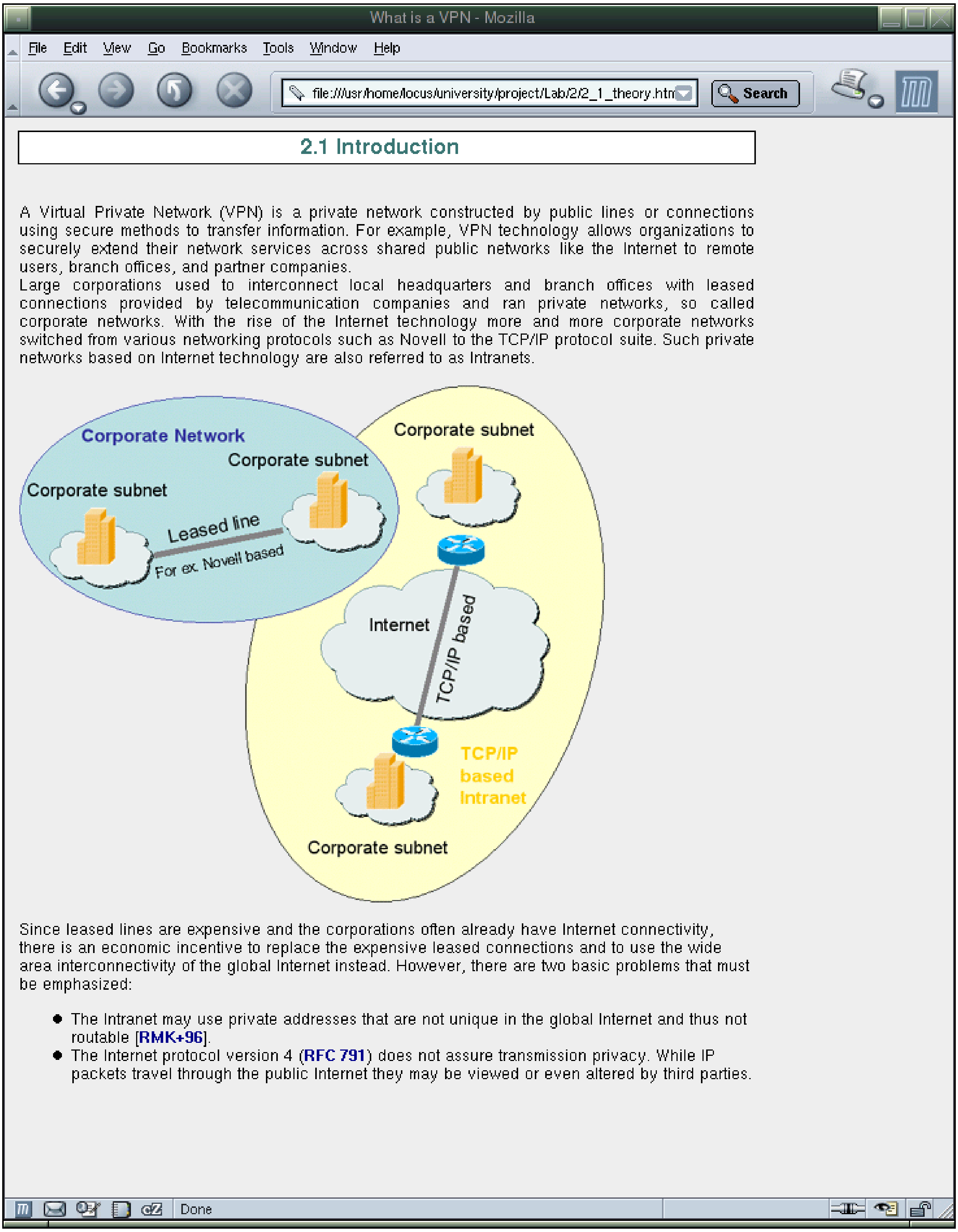
Download chapter 2 as a pdf file:

2 Theoretical Basics

In this section you get introduced into the theoretical basics of IP Security. Read carefully through the provided documents and take the time for understanding what you are reading.

After the theory section there is a readings section where you find more compulsory and recommended readings that can be selected using the Self-Test on the Knowledge page.

Learning in groups is certainly an advantage in many cases, although it cannot replace the monotone study phase where you have to get into a new area. But it definitely helps to overcome context problems in a later phase. WebCT addresses this issue by offering chat rooms, discussion boards and whiteboards. All these tools are open to you and should provide assistance.

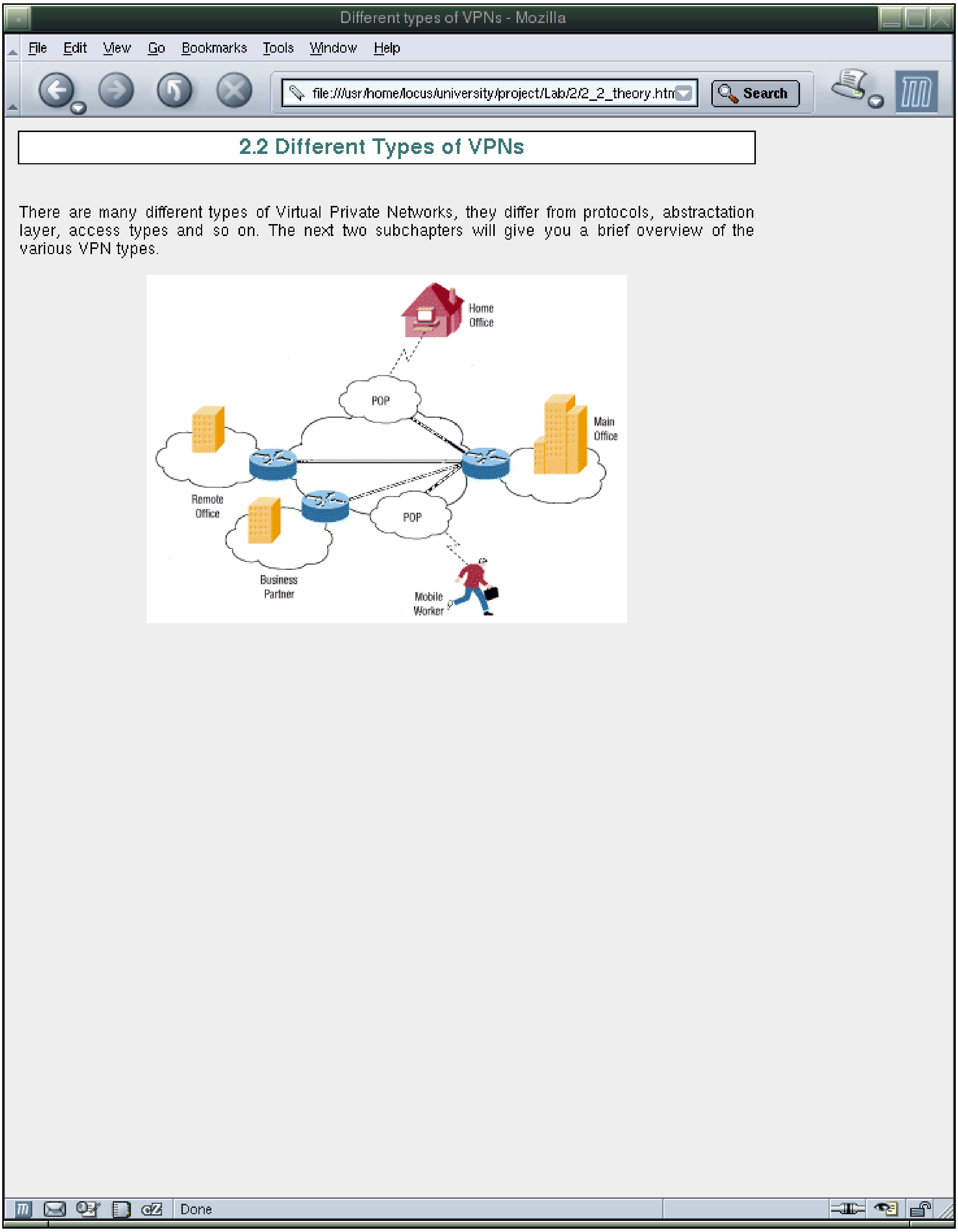

What is a VPN - Mozilla
File Edit View Go Bookmarks Tools Window Help
file:///usr/home/locus/university/project/Lab/2/2_1_theory.htm
Search
Done

2.1 Introduction

A Virtual Private Network (VPN) is a private network constructed by public lines or connections using secure methods to transfer information. For example, VPN technology allows organizations to securely extend their network services across shared public networks like the Internet to remote users, branch offices, and partner companies.
Large corporations used to interconnect local headquarters and branch offices with leased connections provided by telecommunication companies and ran private networks, so called corporate networks. With the rise of the Internet technology more and more corporate networks switched from various networking protocols such as Novell to the TCP/IP protocol suite. Such private networks based on Internet technology are also referred to as Intranets.

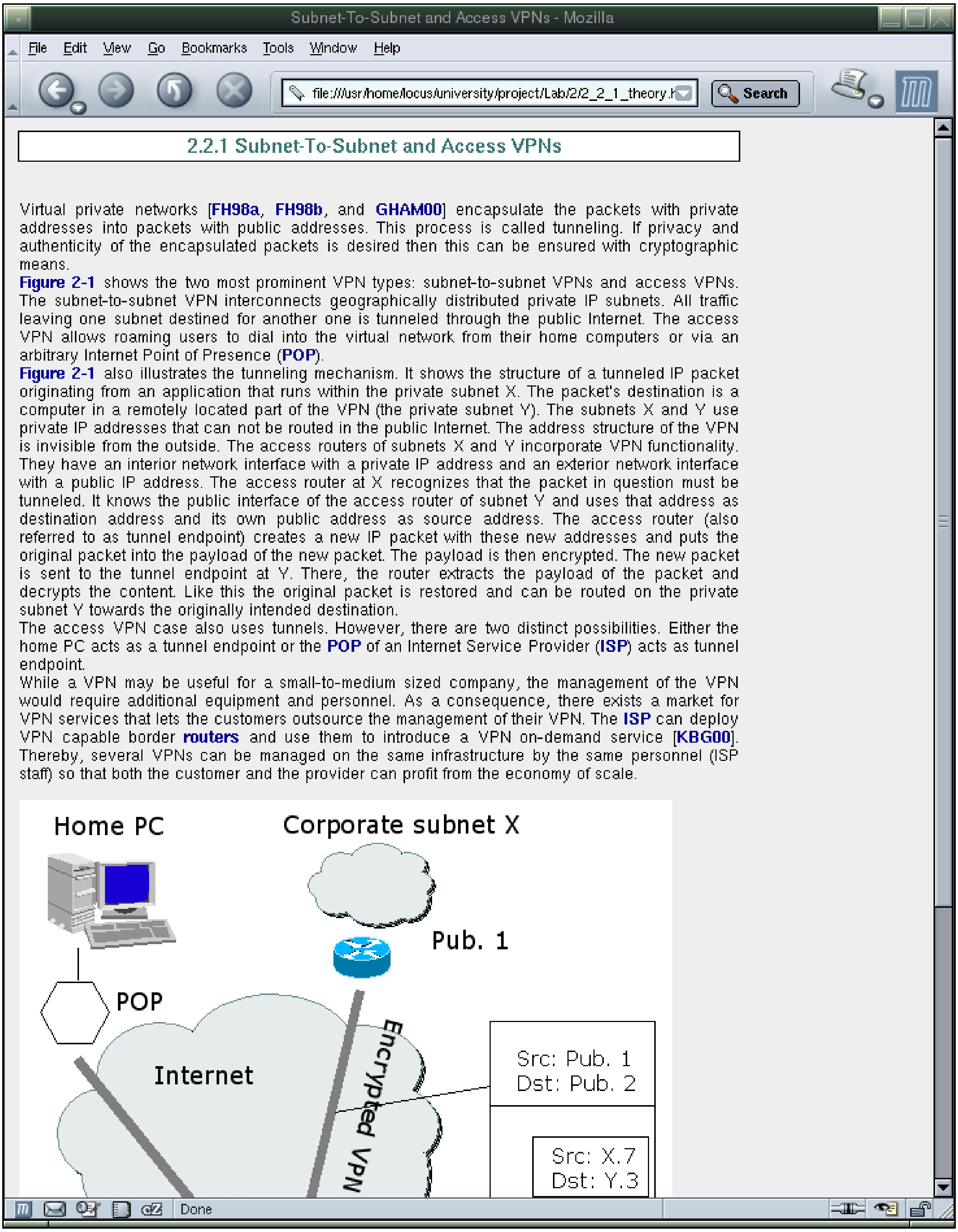
Since leased lines are expensive and the corporations often already have Internet connectivity, there is an economic incentive to replace the expensive leased connections and to use the wide area interconnectivity of the global Internet instead. However, there are two basic problems that must be emphasized:

- The Intranet may use private addresses that are not unique in the global Internet and thus not routable [RMK+96].
- The Internet protocol version 4 (RFC 791) does not assure transmission privacy. While IP packets travel through the public Internet they may be viewed or even altered by third parties.



2.2 Different Types of VPNs

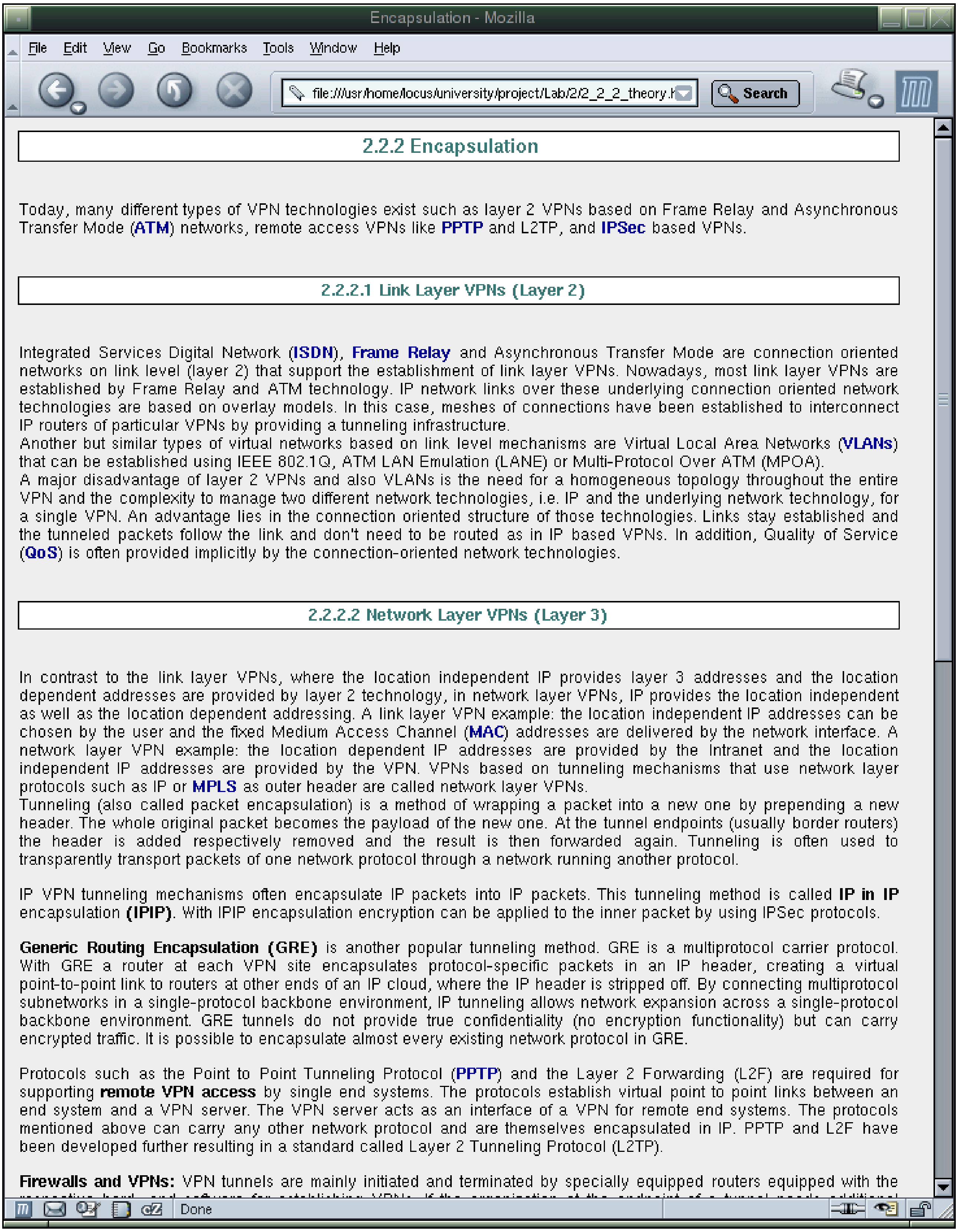
There are many different types of Virtual Private Networks, they differ from protocols, abstractation layer, access types and so on. The next two subchapters will give you a brief overview of the various VPN types.



Subnet-To-Subnet and Access VPNs - Mozilla
File Edit View Go Bookmarks Tools Window Help
file:///usr/home/locus/university/project/Lab/2/2_2_1_theory.h
Search
Done

2.2.1 Subnet-To-Subnet and Access VPNs

Virtual private networks [**FH98a**, **FH98b**, and **GHAM00**] encapsulate the packets with private addresses into packets with public addresses. This process is called tunneling. If privacy and authenticity of the encapsulated packets is desired then this can be ensured with cryptographic means.
Figure 2-1 shows the two most prominent VPN types: subnet-to-subnet VPNs and access VPNs. The subnet-to-subnet VPN interconnects geographically distributed private IP subnets. All traffic leaving one subnet destined for another one is tunneled through the public Internet. The access VPN allows roaming users to dial into the virtual network from their home computers or via an arbitrary Internet Point of Presence (**POP**).
Figure 2-1 also illustrates the tunneling mechanism. It shows the structure of a tunneled IP packet originating from an application that runs within the private subnet X. The packet's destination is a computer in a remotely located part of the VPN (the private subnet Y). The subnets X and Y use private IP addresses that can not be routed in the public Internet. The address structure of the VPN is invisible from the outside. The access routers of subnets X and Y incorporate VPN functionality. They have an interior network interface with a private IP address and an exterior network interface with a public IP address. The access router at X recognizes that the packet in question must be tunneled. It knows the public interface of the access router of subnet Y and uses that address as destination address and its own public address as source address. The access router (also referred to as tunnel endpoint) creates a new IP packet with these new addresses and puts the original packet into the payload of the new packet. The payload is then encrypted. The new packet is sent to the tunnel endpoint at Y. There, the router extracts the payload of the packet and decrypts the content. Like this the original packet is restored and can be routed on the private subnet Y towards the originally intended destination.
The access VPN case also uses tunnels. However, there are two distinct possibilities. Either the home PC acts as a tunnel endpoint or the **POP** of an Internet Service Provider (**ISP**) acts as tunnel endpoint.
While a VPN may be useful for a small-to-medium sized company, the management of the VPN would require additional equipment and personnel. As a consequence, there exists a market for VPN services that lets the customers outsource the management of their VPN. The **ISP** can deploy VPN capable border **routers** and use them to introduce a VPN on-demand service [**KBG00**]. Thereby, several VPNs can be managed on the same infrastructure by the same personnel (ISP staff) so that both the customer and the provider can profit from the economy of scale.


Encapsulation - Mozilla
File Edit View Go Bookmarks Tools Window Help
file:///usr/home/locus/university/project/Lab/2/2_2_2_theory.h
Search
Done

2.2.2 Encapsulation

Today, many different types of VPN technologies exist such as layer 2 VPNs based on Frame Relay and Asynchronous Transfer Mode (**ATM**) networks, remote access VPNs like **PPTP** and L2TP, and **IPSec** based VPNs.

2.2.2.1 Link Layer VPNs (Layer 2)

Integrated Services Digital Network (**ISDN**), **Frame Relay** and Asynchronous Transfer Mode are connection oriented networks on link level (layer 2) that support the establishment of link layer VPNs. Nowadays, most link layer VPNs are established by Frame Relay and ATM technology. IP network links over these underlying connection oriented network technologies are based on overlay models. In this case, meshes of connections have been established to interconnect IP routers of particular VPNs by providing a tunneling infrastructure.
Another but similar types of virtual networks based on link level mechanisms are Virtual Local Area Networks (**VLANs**) that can be established using IEEE 802.1Q, ATM LAN Emulation (LANE) or Multi-Protocol Over ATM (MPOA).
A major disadvantage of layer 2 VPNs and also VLANs is the need for a homogeneous topology throughout the entire VPN and the complexity to manage two different network technologies, i.e. IP and the underlying network technology, for a single VPN. An advantage lies in the connection oriented structure of those technologies. Links stay established and the tunneled packets follow the link and don't need to be routed as in IP based VPNs. In addition, Quality of Service (**QoS**) is often provided implicitly by the connection-oriented network technologies.

2.2.2.2 Network Layer VPNs (Layer 3)

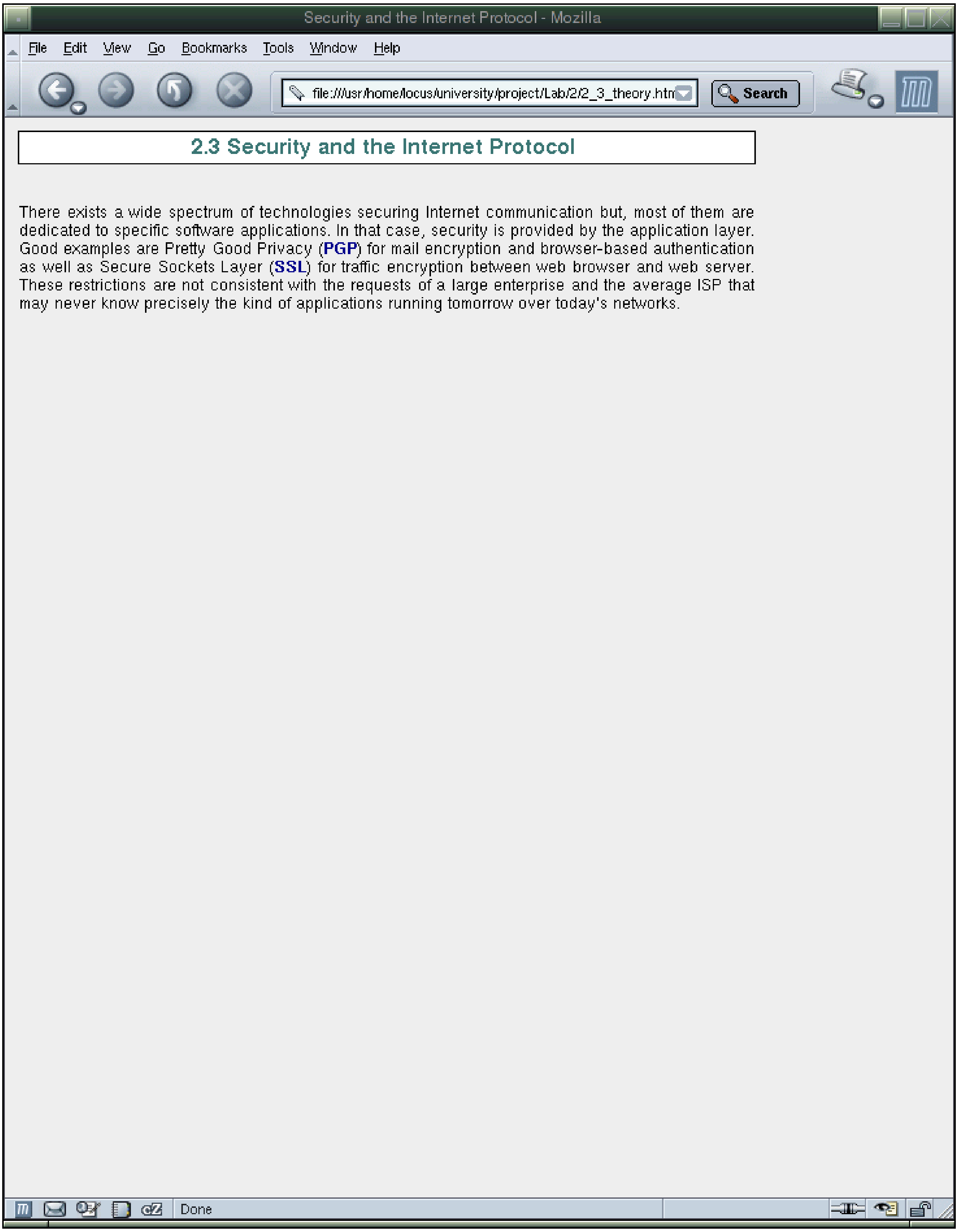
In contrast to the link layer VPNs, where the location independent IP provides layer 3 addresses and the location dependent addresses are provided by layer 2 technology, in network layer VPNs, IP provides the location independent as well as the location dependent addressing. A link layer VPN example: the location independent IP addresses can be chosen by the user and the fixed Medium Access Channel (**MAC**) addresses are delivered by the network interface. A network layer VPN example: the location dependent IP addresses are provided by the Intranet and the location independent IP addresses are provided by the VPN. VPNs based on tunneling mechanisms that use network layer protocols such as IP or **MPLS** as outer header are called network layer VPNs.
Tunneling (also called packet encapsulation) is a method of wrapping a packet into a new one by prepending a new header. The whole original packet becomes the payload of the new one. At the tunnel endpoints (usually border routers) the header is added respectively removed and the result is then forwarded again. Tunneling is often used to transparently transport packets of one network protocol through a network running another protocol.

IP VPN tunneling mechanisms often encapsulate IP packets into IP packets. This tunneling method is called **IP in IP** encapsulation **(IPIP)**. With IPIP encapsulation encryption can be applied to the inner packet by using IPSec protocols.

Generic Routing Encapsulation (GRE) is another popular tunneling method. GRE is a multiprotocol carrier protocol. With GRE a router at each VPN site encapsulates protocol-specific packets in an IP header, creating a virtual point-to-point link to routers at other ends of an IP cloud, where the IP header is stripped off. By connecting multiprotocol subnetworks in a single-protocol backbone environment, IP tunneling allows network expansion across a single-protocol backbone environment. GRE tunnels do not provide true confidentiality (no encryption functionality) but can carry encrypted traffic. It is possible to encapsulate almost every existing network protocol in GRE.

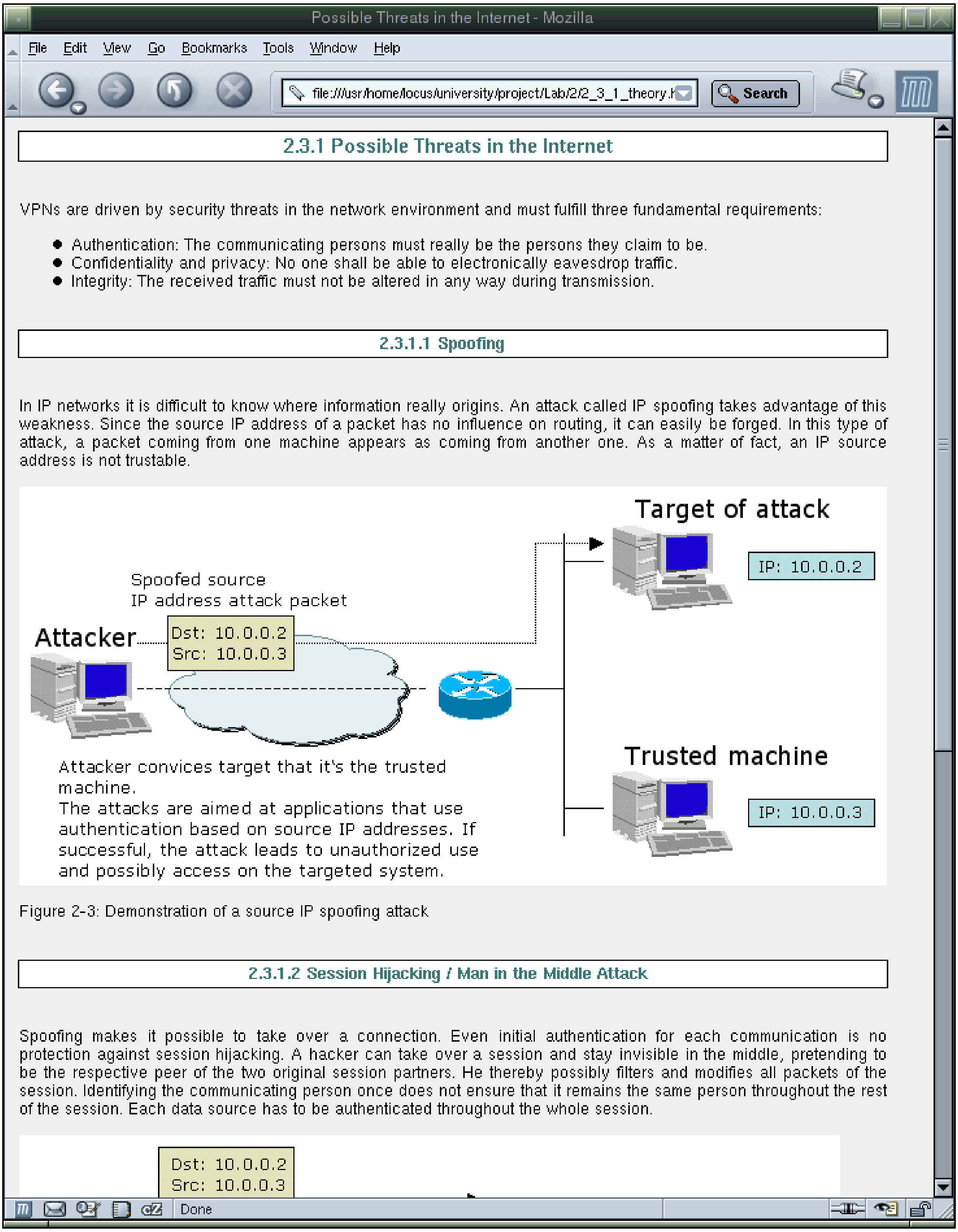
Protocols such as the Point to Point Tunneling Protocol (**PPTP**) and the Layer 2 Forwarding (L2F) are required for supporting **remote VPN access** by single end systems. The protocols establish virtual point to point links between an end system and a VPN server. The VPN server acts as an interface of a VPN for remote end systems. The protocols mentioned above can carry any other network protocol and are themselves encapsulated in IP. PPTP and L2F have been developed further resulting in a standard called Layer 2 Tunneling Protocol (L2TP).

Firewalls and VPNs: VPN tunnels are mainly initiated and terminated by specially equipped routers equipped with the


Security and the Internet Protocol - Mozilla
File Edit View Go Bookmarks Tools Window Help
file:///usr/home/locus/university/project/Lab/2/2_3_theory.htm
Search
Done

2.3 Security and the Internet Protocol

There exists a wide spectrum of technologies securing Internet communication but, most of them are dedicated to specific software applications. In that case, security is provided by the application layer. Good examples are Pretty Good Privacy (**PGP**) for mail encryption and browser-based authentication as well as Secure Sockets Layer (**SSL**) for traffic encryption between web browser and web server. These restrictions are not consistent with the requests of a large enterprise and the average ISP that may never know precisely the kind of applications running tomorrow over today's networks.


Possible Threats in the Internet - Mozilla
File Edit View Go Bookmarks Tools Window Help
file:///usr/home/locus/university/project/Lab/2/2_3_1_theory.h
Search
Done

2.3.1 Possible Threats in the Internet

VPNs are driven by security threats in the network environment and must fulfill three fundamental requirements:

- Authentication: The communicating persons must really be the persons they claim to be.
- Confidentiality and privacy: No one shall be able to electronically eavesdrop traffic.
- Integrity: The received traffic must not be altered in any way during transmission.

2.3.1.1 Spoofing

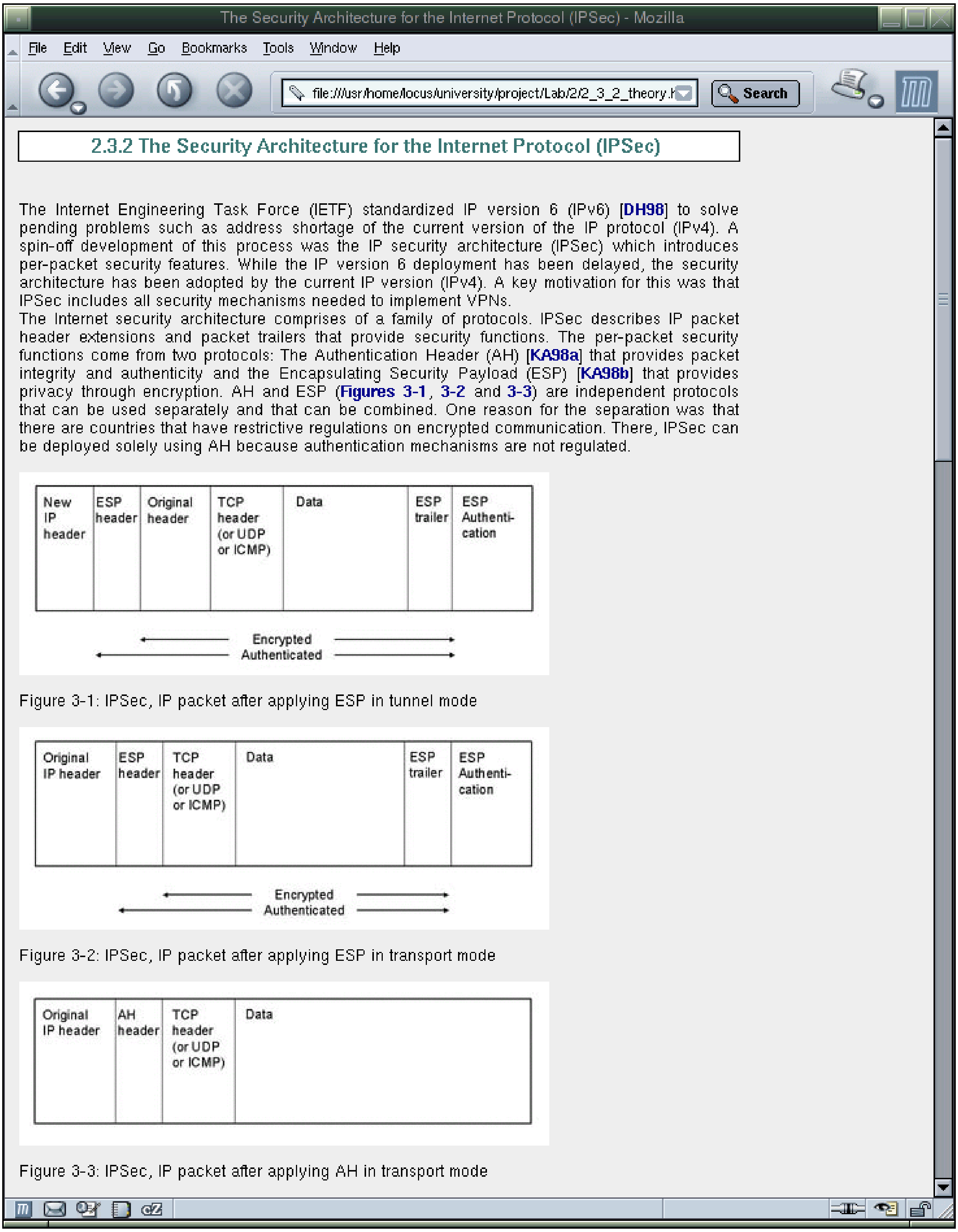
In IP networks it is difficult to know where information really origins. An attack called IP spoofing takes advantage of this weakness. Since the source IP address of a packet has no influence on routing, it can easily be forged. In this type of attack, a packet coming from one machine appears as coming from another one. As a matter of fact, an IP source address is not trustable.

Attacker convices target that it's the trusted machine.
The attacks are aimed at applications that use authentication based on source IP addresses. If successful, the attack leads to unauthorized use and possibly access on the targeted system.

Figure 2-3: Demonstration of a source IP spoofing attack

2.3.1.2 Session Hijacking / Man in the Middle Attack

Spoofing makes it possible to take over a connection. Even initial authentication for each communication is no protection against session hijacking. A hacker can take over a session and stay invisible in the middle, pretending to be the respective peer of the two original session partners. He thereby possibly filters and modifies all packets of the session. Identifying the communicating person once does not ensure that it remains the same person throughout the rest of the session. Each data source has to be authenticated throughout the whole session.



The Security Architecture for the Internet Protocol (IPSec) - Mozilla
File Edit View Go Bookmarks Tools Window Help
file:///usr/home/locus/university/project/Lab/2/2_3_2_theory.h
Search

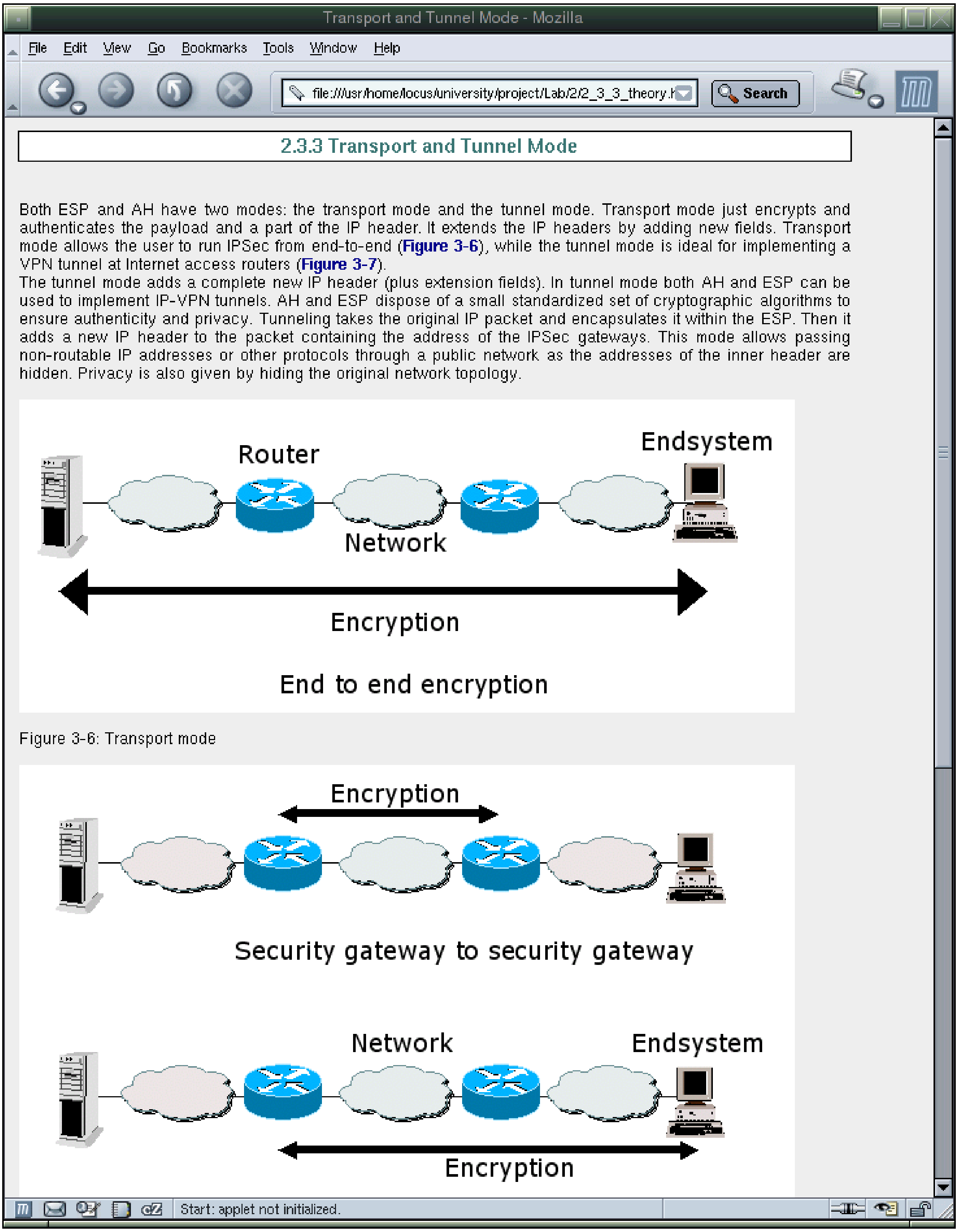
2.3.2 The Security Architecture for the Internet Protocol (IPSec)

The Internet Engineering Task Force (IETF) standardized IP version 6 (IPv6) [DH98] to solve pending problems such as address shortage of the current version of the IP protocol (IPv4). A spin-off development of this process was the IP security architecture (IPSec) which introduces per-packet security features. While the IP version 6 deployment has been delayed, the security architecture has been adopted by the current IP version (IPv4). A key motivation for this was that IPSec includes all security mechanisms needed to implement VPNs.
The Internet security architecture comprises of a family of protocols. IPSec describes IP packet header extensions and packet trailers that provide security functions. The per-packet security functions come from two protocols: The Authentication Header (AH) [KA98a] that provides packet integrity and authenticity and the Encapsulating Security Payload (ESP) [KA98b] that provides privacy through encryption. AH and ESP (Figures 3-1 , 3-2 and 3-3) are independent protocols that can be used separately and that can be combined. One reason for the separation was that there are countries that have restrictive regulations on encrypted communication. There, IPSec can be deployed solely using AH because authentication mechanisms are not regulated.

Figure 3-1: IPSec, IP packet after applying ESP in tunnel mode

Figure 3-2: IPSec, IP packet after applying ESP in transport mode

Figure 3-3: IPSec, IP packet after applying AH in transport mode

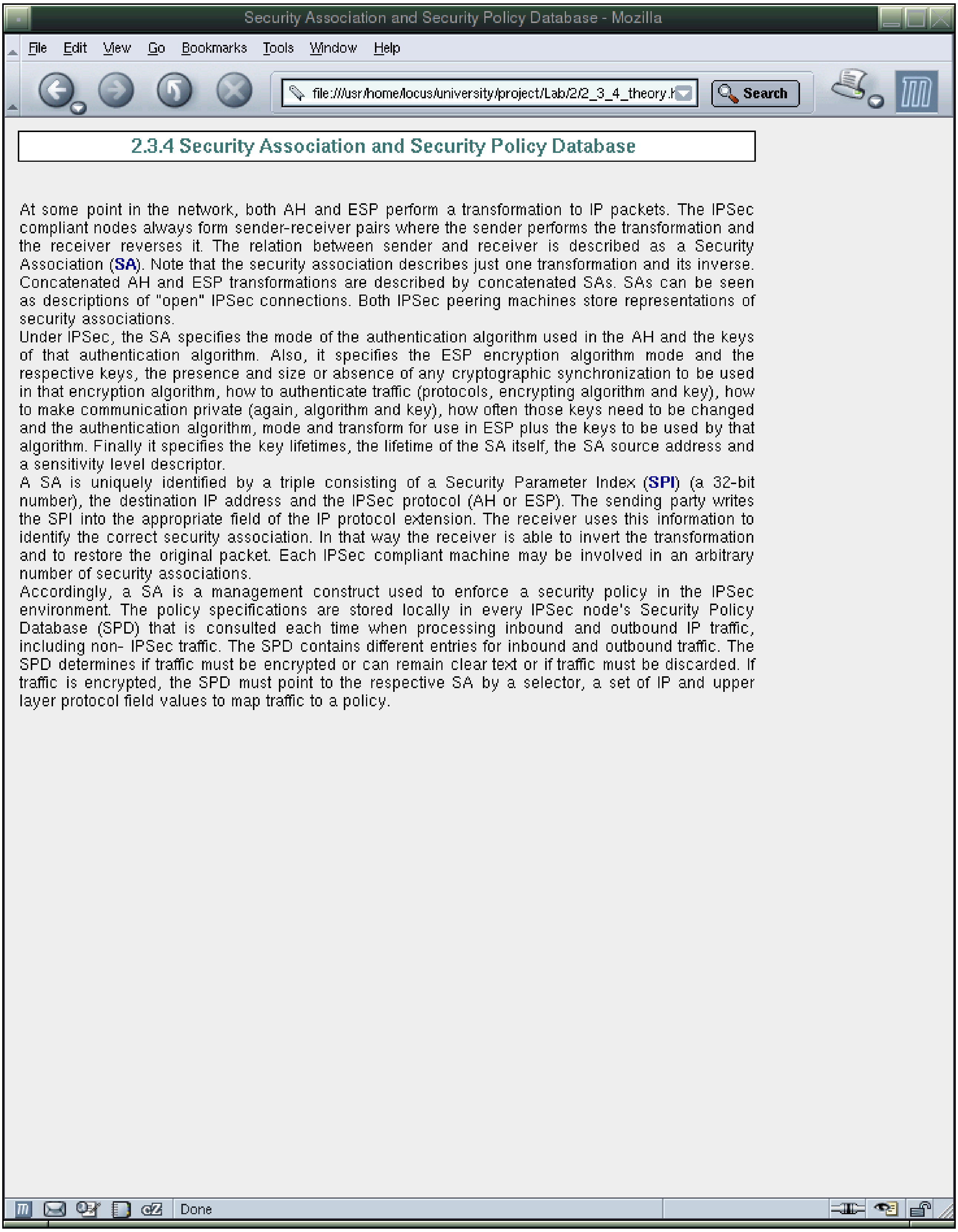

Transport and Tunnel Mode - Mozilla
File
Edit
View
Go
Bookmarks
Tools
Window
Help
file:///usr/home/locus/university/project/Lab/2/2_3_3_theory.h
Search

2.3.3 Transport and Tunnel Mode

Both ESP and AH have two modes: the transport mode and the tunnel mode. Transport mode just encrypts and authenticates the payload and a part of the IP header. It extends the IP headers by adding new fields. Transport mode allows the user to run IPSec from end-to-end (**Figure 3-6**), while the tunnel mode is ideal for implementing a VPN tunnel at Internet access routers (**Figure 3-7**).
The tunnel mode adds a complete new IP header (plus extension fields). In tunnel mode both AH and ESP can be used to implement IP-VPN tunnels. AH and ESP dispose of a small standardized set of cryptographic algorithms to ensure authenticity and privacy. Tunneling takes the original IP packet and encapsulates it within the ESP. Then it adds a new IP header to the packet containing the address of the IPSec gateways. This mode allows passing non-routable IP addresses or other protocols through a public network as the addresses of the inner header are hidden. Privacy is also given by hiding the original network topology.

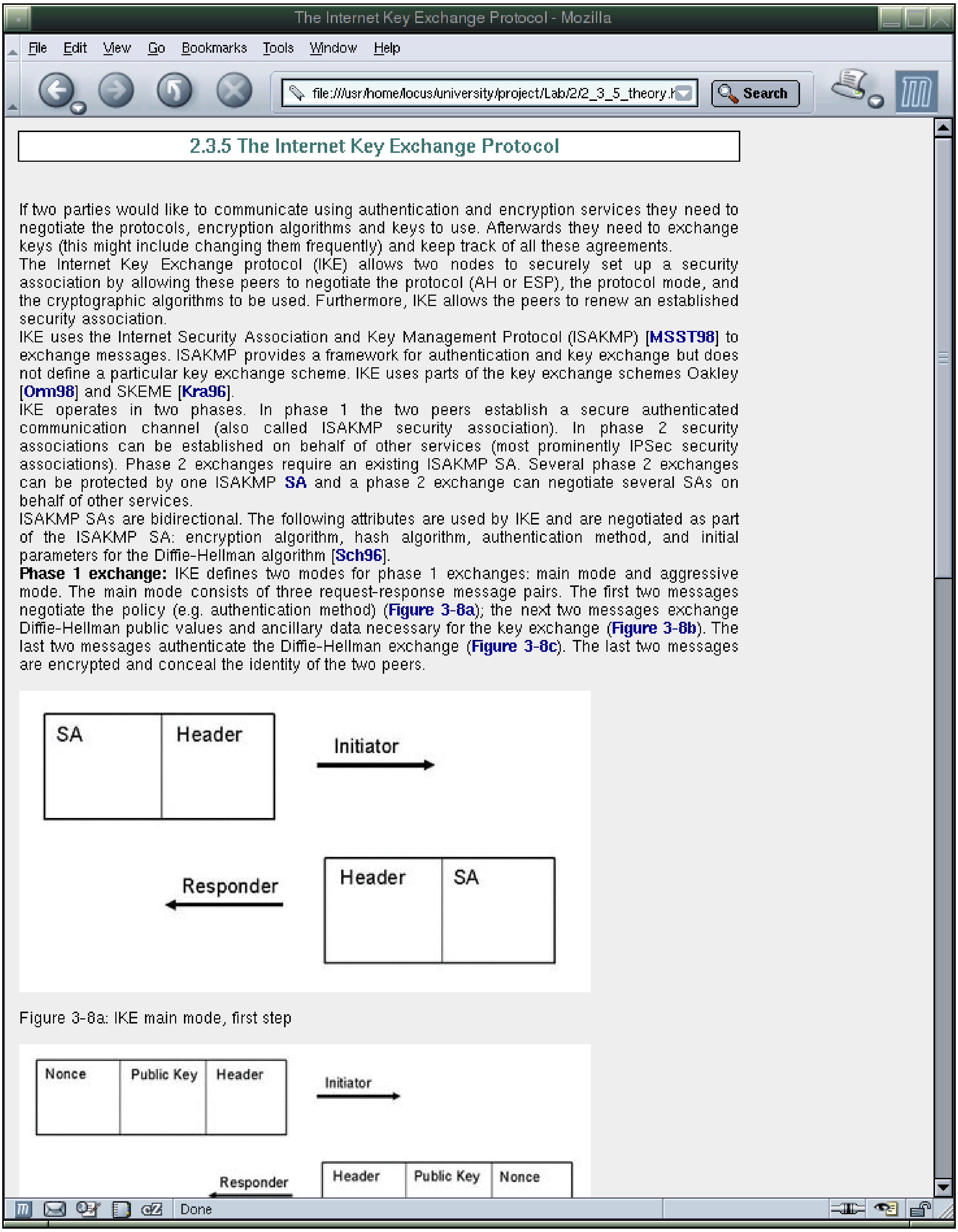
Figure 3-6: Transport mode

Start: applet not initialized.


Security Association and Security Policy Database - Mozilla
File Edit View Go Bookmarks Tools Window Help
file:///usr/home/locus/university/project/Lab/2/2_3_4_theory.h
Search
Done

2.3.4 Security Association and Security Policy Database

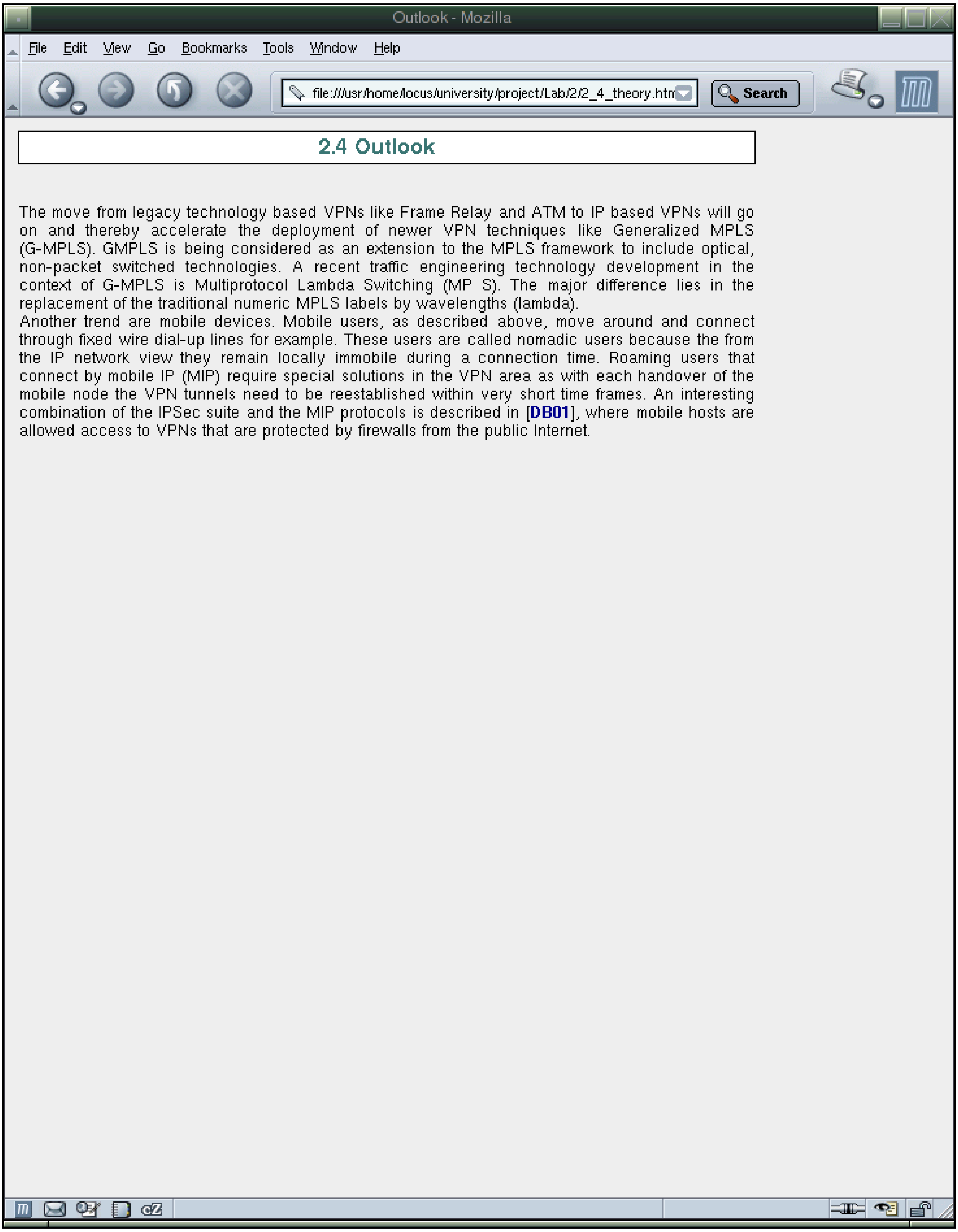
At some point in the network, both AH and ESP perform a transformation to IP packets. The IPSec compliant nodes always form sender-receiver pairs where the sender performs the transformation and the receiver reverses it. The relation between sender and receiver is described as a Security Association (**SA**). Note that the security association describes just one transformation and its inverse. Concatenated AH and ESP transformations are described by concatenated SAs. SAs can be seen as descriptions of "open" IPSec connections. Both IPSec peering machines store representations of security associations.
Under IPSec, the SA specifies the mode of the authentication algorithm used in the AH and the keys of that authentication algorithm. Also, it specifies the ESP encryption algorithm mode and the respective keys, the presence and size or absence of any cryptographic synchronization to be used in that encryption algorithm, how to authenticate traffic (protocols, encrypting algorithm and key), how to make communication private (again, algorithm and key), how often those keys need to be changed and the authentication algorithm, mode and transform for use in ESP plus the keys to be used by that algorithm. Finally it specifies the key lifetimes, the lifetime of the SA itself, the SA source address and a sensitivity level descriptor.
A SA is uniquely identified by a triple consisting of a Security Parameter Index (**SPI**) (a 32-bit number), the destination IP address and the IPSec protocol (AH or ESP). The sending party writes the SPI into the appropriate field of the IP protocol extension. The receiver uses this information to identify the correct security association. In that way the receiver is able to invert the transformation and to restore the original packet. Each IPSec compliant machine may be involved in an arbitrary number of security associations.
Accordingly, a SA is a management construct used to enforce a security policy in the IPSec environment. The policy specifications are stored locally in every IPSec node's Security Policy Database (SPD) that is consulted each time when processing inbound and outbound IP traffic, including non- IPSec traffic. The SPD contains different entries for inbound and outbound traffic. The SPD determines if traffic must be encrypted or can remain clear text or if traffic must be discarded. If traffic is encrypted, the SPD must point to the respective SA by a selector, a set of IP and upper layer protocol field values to map traffic to a policy.


The Internet Key Exchange Protocol - Mozilla
File Edit View Go Bookmarks Tools Window Help
file:///usr/home/locus/university/project/Lab/2/2_3_5_theory.h
Search
Done

2.3.5 The Internet Key Exchange Protocol

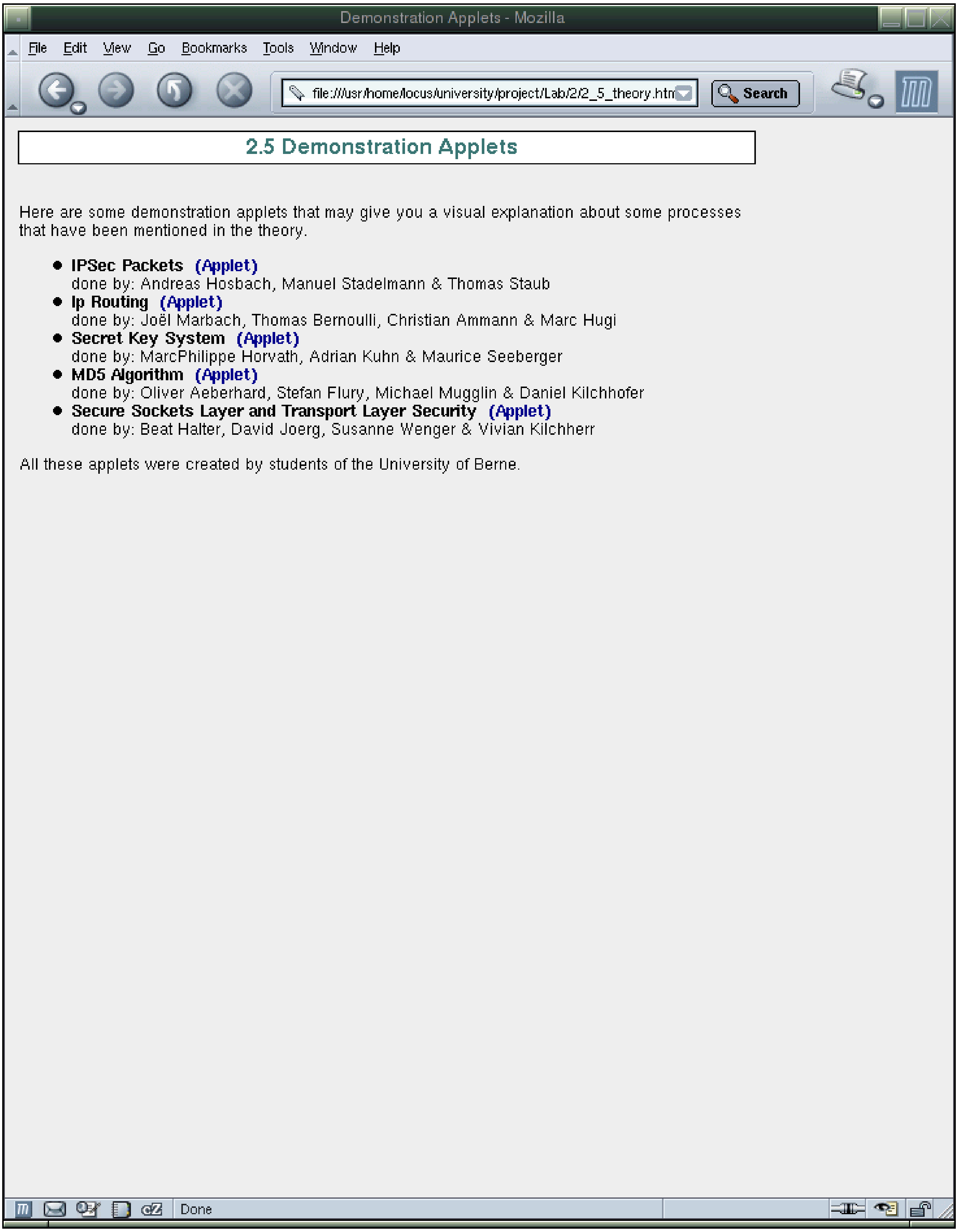
If two parties would like to communicate using authentication and encryption services they need to negotiate the protocols, encryption algorithms and keys to use. Afterwards they need to exchange keys (this might include changing them frequently) and keep track of all these agreements.
The Internet Key Exchange protocol (IKE) allows two nodes to securely set up a security association by allowing these peers to negotiate the protocol (AH or ESP), the protocol mode, and the cryptographic algorithms to be used. Furthermore, IKE allows the peers to renew an established security association.
IKE uses the Internet Security Association and Key Management Protocol (ISAKMP) [MSST98] to exchange messages. ISAKMP provides a framework for authentication and key exchange but does not define a particular key exchange scheme. IKE uses parts of the key exchange schemes Oakley [Orm98] and SKEME [Kra96].
IKE operates in two phases. In phase 1 the two peers establish a secure authenticated communication channel (also called ISAKMP security association). In phase 2 security associations can be established on behalf of other services (most prominently IPSec security associations). Phase 2 exchanges require an existing ISAKMP SA. Several phase 2 exchanges can be protected by one ISAKMP SA and a phase 2 exchange can negotiate several SAs on behalf of other services.
ISAKMP SAs are bidirectional. The following attributes are used by IKE and are negotiated as part of the ISAKMP SA: encryption algorithm, hash algorithm, authentication method, and initial parameters for the Diffie-Hellman algorithm [Sch96].
Phase 1 exchange: IKE defines two modes for phase 1 exchanges: main mode and aggressive mode. The main mode consists of three request-response message pairs. The first two messages negotiate the policy (e.g. authentication method) (Figure 3-8a); the next two messages exchange Diffie-Hellman public values and ancillary data necessary for the key exchange (Figure 3-8b). The last two messages authenticate the Diffie-Hellman exchange (Figure 3-8c). The last two messages are encrypted and conceal the identity of the two peers.

Figure 3-8a: IKE main mode, first step


Outlook - Mozilla
File Edit View Go Bookmarks Tools Window Help
file:///usr/home/locus/university/project/Lab/2/2_4_theory.htm
Search

2.4 Outlook

The move from legacy technology based VPNs like Frame Relay and ATM to IP based VPNs will go on and thereby accelerate the deployment of newer VPN techniques like Generalized MPLS (G-MPLS). GMPLS is being considered as an extension to the MPLS framework to include optical, non-packet switched technologies. A recent traffic engineering technology development in the context of G-MPLS is Multiprotocol Lambda Switching (MP S). The major difference lies in the replacement of the traditional numeric MPLS labels by wavelengths (lambda).
Another trend are mobile devices. Mobile users, as described above, move around and connect through fixed wire dial-up lines for example. These users are called nomadic users because the from the IP network view they remain locally immobile during a connection time. Roaming users that connect by mobile IP (MIP) require special solutions in the VPN area as with each handover of the mobile node the VPN tunnels need to be reestablished within very short time frames. An interesting combination of the IPSec suite and the MIP protocols is described in [DB01], where mobile hosts are allowed access to VPNs that are protected by firewalls from the public Internet.

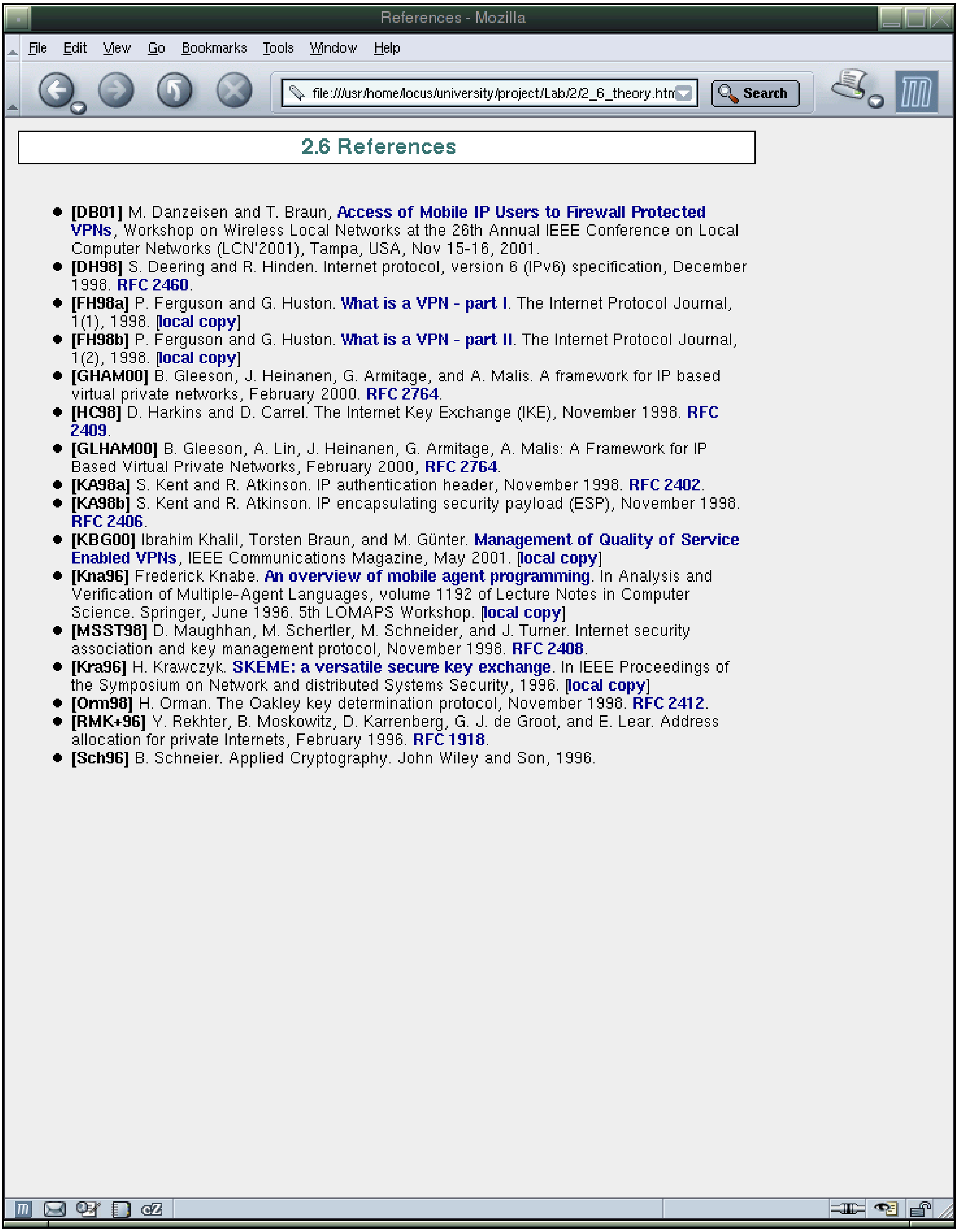

Demonstration Applets - Mozilla
File Edit View Go Bookmarks Tools Window Help
file:///usr/home/locus/university/project/Lab/2/2_5_theory.htm
Search
Done

2.5 Demonstration Applets

Here are some demonstration applets that may give you a visual explanation about some processes that have been mentioned in the theory.

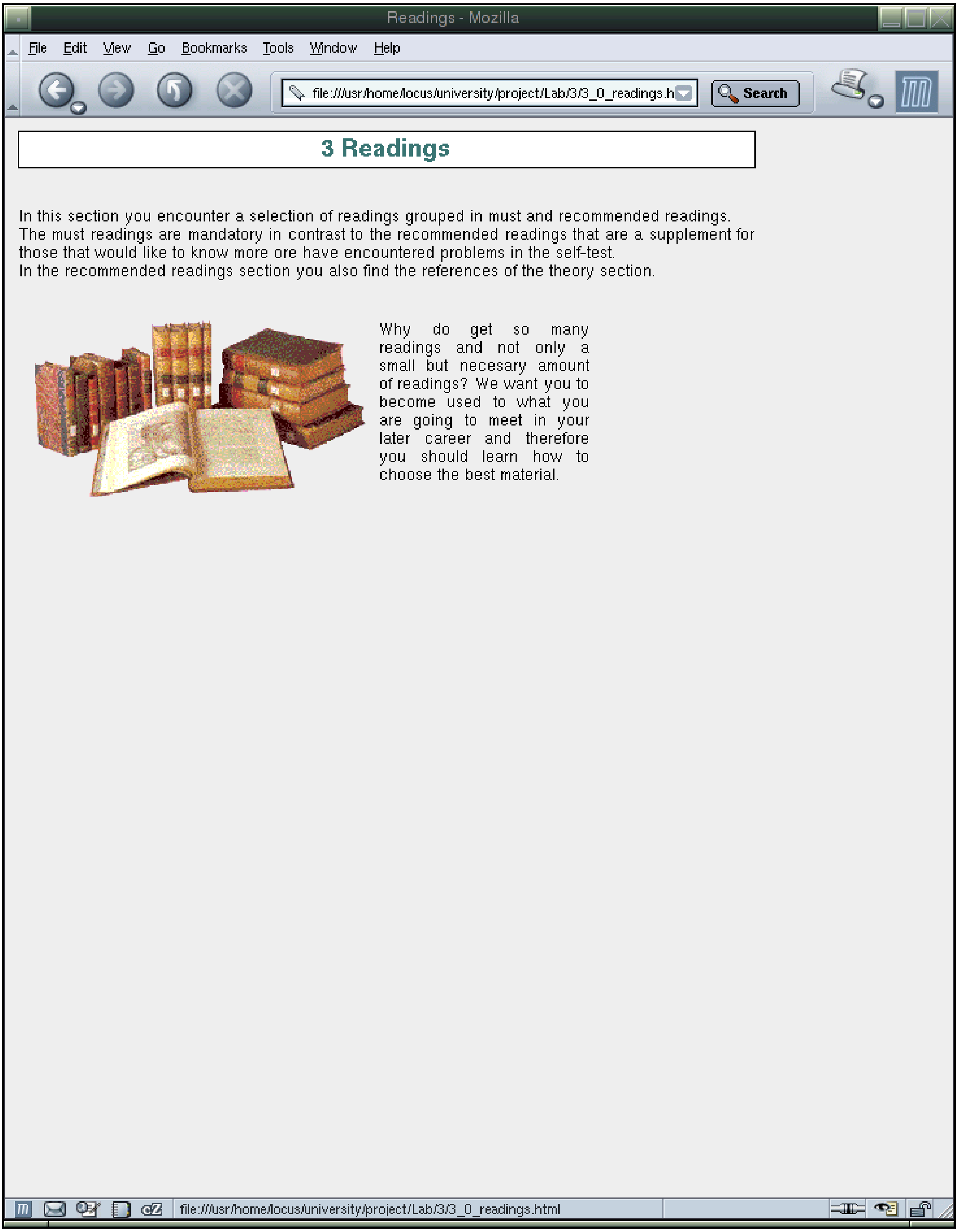
- **IPSec Packets** **(Applet)**
  done by: Andreas Hosbach, Manuel Stadelmann & Thomas Staub
- **Ip Routing** **(Applet)**
  done by: Joël Marbach, Thomas Bernoulli, Christian Ammann & Marc Hugi
- **Secret Key System** **(Applet)**
  done by: MarcPhilippe Horvath, Adrian Kuhn & Maurice Seeberger
- **MD5 Algorithm** **(Applet)**
  done by: Oliver Aeberhard, Stefan Flury, Michael Mugglin & Daniel Kilchhofer
- **Secure Sockets Layer and Transport Layer Security** **(Applet)**
  done by: Beat Halter, David Joerg, Susanne Wenger & Vivian Kilchherr

All these applets were created by students of the University of Berne.


References - Mozilla
File Edit View Go Bookmarks Tools Window Help
file:///usr/home/locus/university/project/Lab/2/2_6_theory.htm
Search

2.6 References

- **[DB01]** M. Danzeisen and T. Braun, **Access of Mobile IP Users to Firewall Protected VPNs**, Workshop on Wireless Local Networks at the 26th Annual IEEE Conference on Local Computer Networks (LCN'2001), Tampa, USA, Nov 15-16, 2001.
- **[DH98]** S. Deering and R. Hinden. Internet protocol, version 6 (IPv6) specification, December 1998. **RFC 2460**.
- **[FH98a]** P. Ferguson and G. Huston. **What is a VPN - part I**. The Internet Protocol Journal, 1(1), 1998. [**local copy**]
- **[FH98b]** P. Ferguson and G. Huston. **What is a VPN - part II**. The Internet Protocol Journal, 1(2), 1998. [**local copy**]
- **[GHAM00]** B. Gleeson, J. Heinanen, G. Armitage, and A. Malis. A framework for IP based virtual private networks, February 2000. **RFC 2764**.
- **[HC98]** D. Harkins and D. Carrel. The Internet Key Exchange (IKE), November 1998. **RFC 2409**.
- **[GLHAM00]** B. Gleeson, A. Lin, J. Heinanen, G. Armitage, A. Malis: A Framework for IP Based Virtual Private Networks, February 2000, **RFC 2764**.
- **[KA98a]** S. Kent and R. Atkinson. IP authentication header, November 1998. **RFC 2402**.
- **[KA98b]** S. Kent and R. Atkinson. IP encapsulating security payload (ESP), November 1998. **RFC 2406**.
- **[KBG00]** Ibrahim Khalil, Torsten Braun, and M. Günter. **Management of Quality of Service Enabled VPNs**, IEEE Communications Magazine, May 2001. [**local copy**]
- **[Kna96]** Frederick Knabe. **An overview of mobile agent programming**. In Analysis and Verification of Multiple-Agent Languages, volume 1192 of Lecture Notes in Computer Science. Springer, June 1996. 5th LOMAPS Workshop. [**local copy**]
- **[MSST98]** D. Maughhan, M. Schertler, M. Schneider, and J. Turner. Internet security association and key management protocol, November 1998. **RFC 2408**.
- **[Kra96]** H. Krawczyk. **SKEME: a versatile secure key exchange**. In IEEE Proceedings of the Symposium on Network and distributed Systems Security, 1996. [**local copy**]
- **[Orn98]** H. Orman. The Oakley key determination protocol, November 1998. **RFC 2412**.
- **[RMK+96]** Y. Rekhter, B. Moskowitz, D. Karrenberg, G. J. de Groot, and E. Lear. Address allocation for private Internets, February 1996. **RFC 1918**.
- **[Sch96]** B. Schneier. Applied Cryptography. John Wiley and Son, 1996.

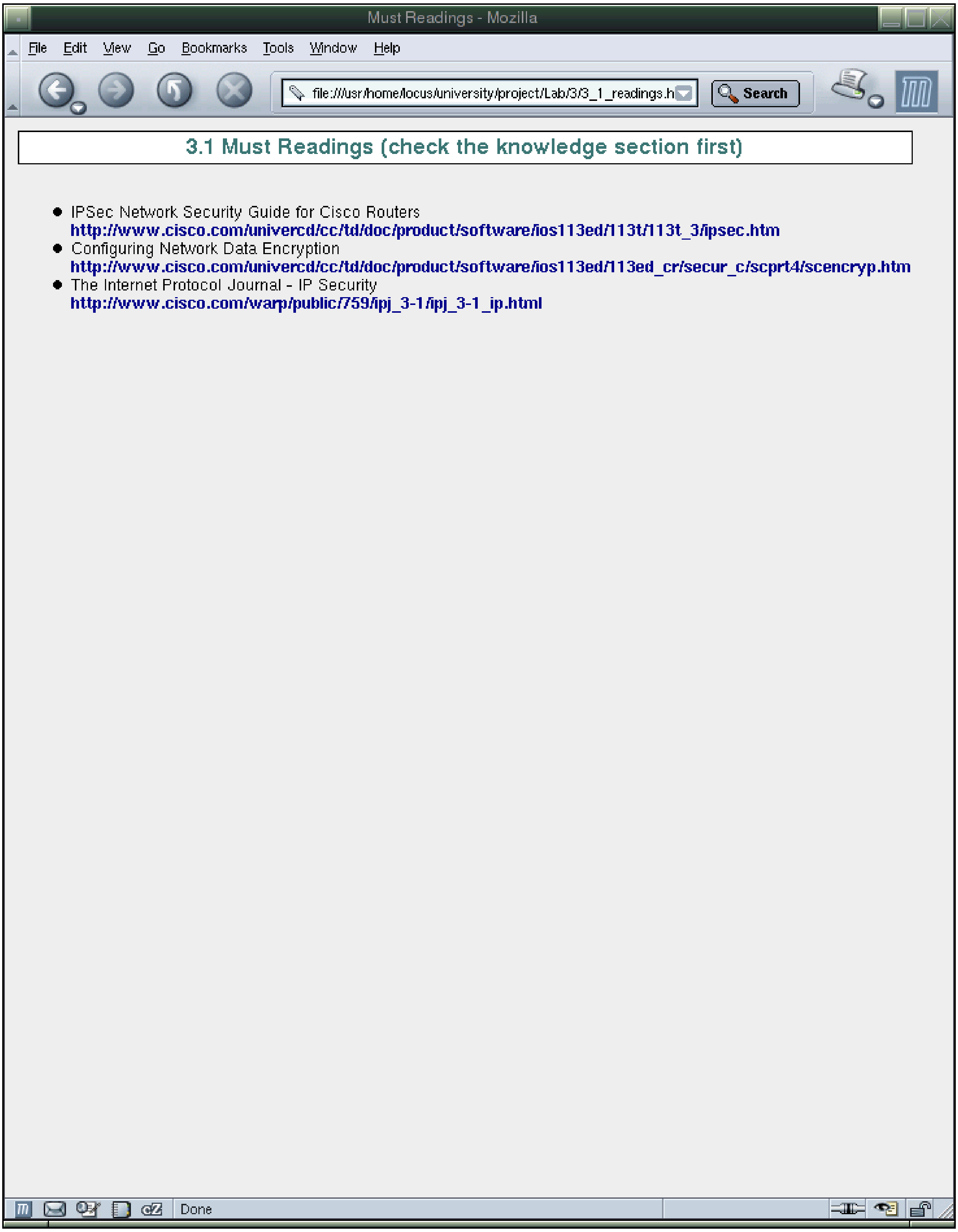


Readings - Mozilla
File Edit View Go Bookmarks Tools Window Help
file:///usr/home/locus/university/project/Lab/3/3_0_readings.h
Search
file:///usr/home/locus/university/project/Lab/3/3_0_readings.html

3 Readings

In this section you encounter a selection of readings grouped in must and recommended readings.
The must readings are mandatory in contrast to the recommended readings that are a supplement for those that would like to know more ore have encountered problems in the self-test.
In the recommended readings section you also find the references of the theory section.

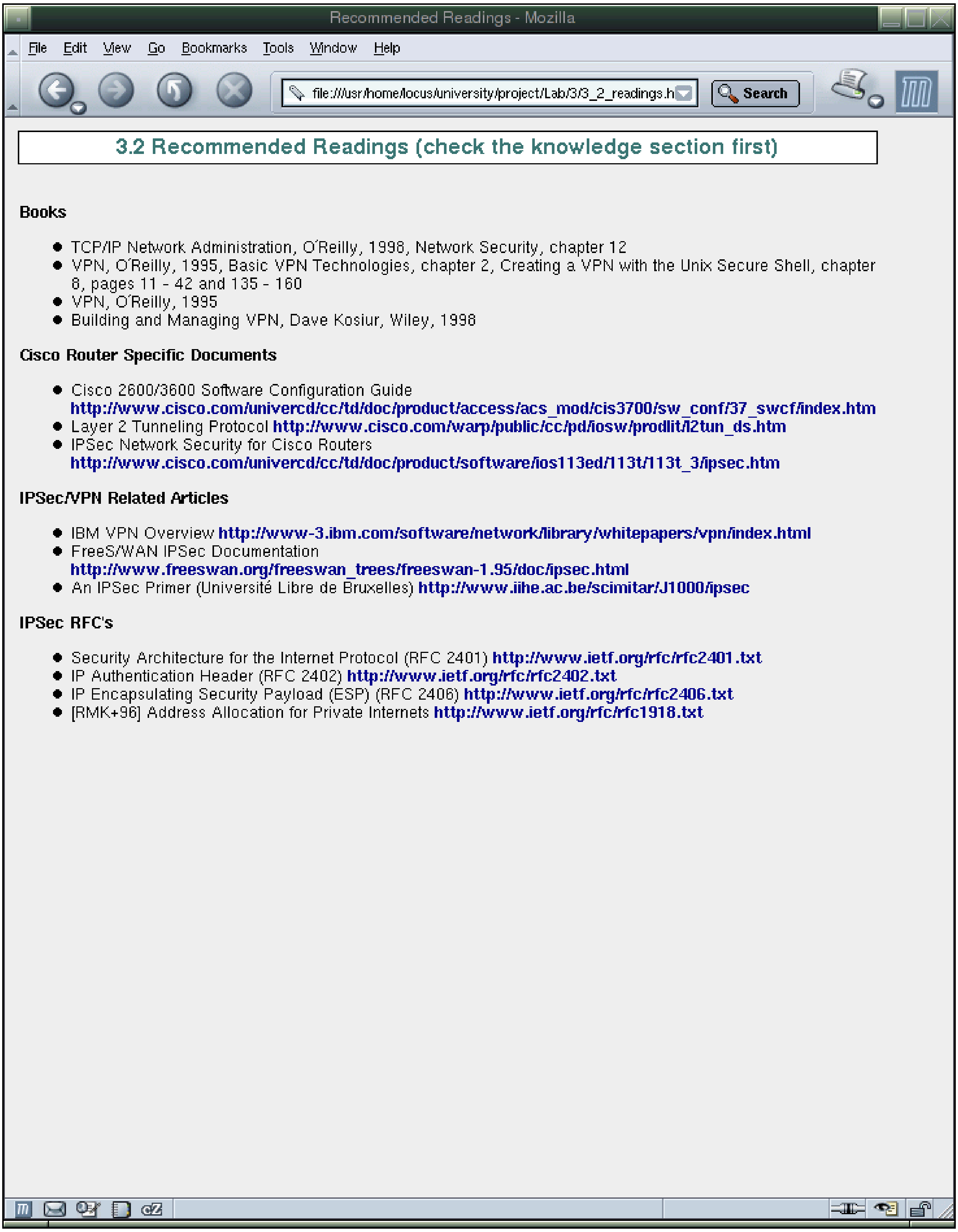
Why do get so many readings and not only a small but necesary amount of readings? We want you to become used to what you are going to meet in your later career and therefore you should learn how to choose the best material.



Must Readings - Mozilla
File Edit View Go Bookmarks Tools Window Help
file:///usr/home/locus/university/project/Lab/3/3_1_readings.h
Search
Done

3.1 Must Readings (check the knowledge section first)

- IPSec Network Security Guide for Cisco Routers
  http://www.cisco.com/univercd/cc/td/doc/product/software/ios113ed/113t/113t_3/ipsec.htm
- Configuring Network Data Encryption
  http://www.cisco.com/univercd/cc/td/doc/product/software/ios113ed/113ed_cr/secur_c/scprt4/scencryp.htm
- The Internet Protocol Journal - IP Security
  http://www.cisco.com/warp/public/759/ipj_3-1/ipj_3-1_ip.html



Recommended Readings - Mozilla
File Edit View Go Bookmarks Tools Window Help
file:///usr/home/locus/university/project/Lab/3/3_2_readings.h
Search

3.2 Recommended Readings (check the knowledge section first)

Books

- TCP/IP Network Administration, O´Reilly, 1998, Network Security, chapter 12
- VPN, O´Reilly, 1995, Basic VPN Technologies, chapter 2, Creating a VPN with the Unix Secure Shell, chapter 8, pages 11 - 42 and 135 - 160
- VPN, O´Reilly, 1995
- Building and Managing VPN, Dave Kosiur, Wiley, 1998

Cisco Router Specific Documents

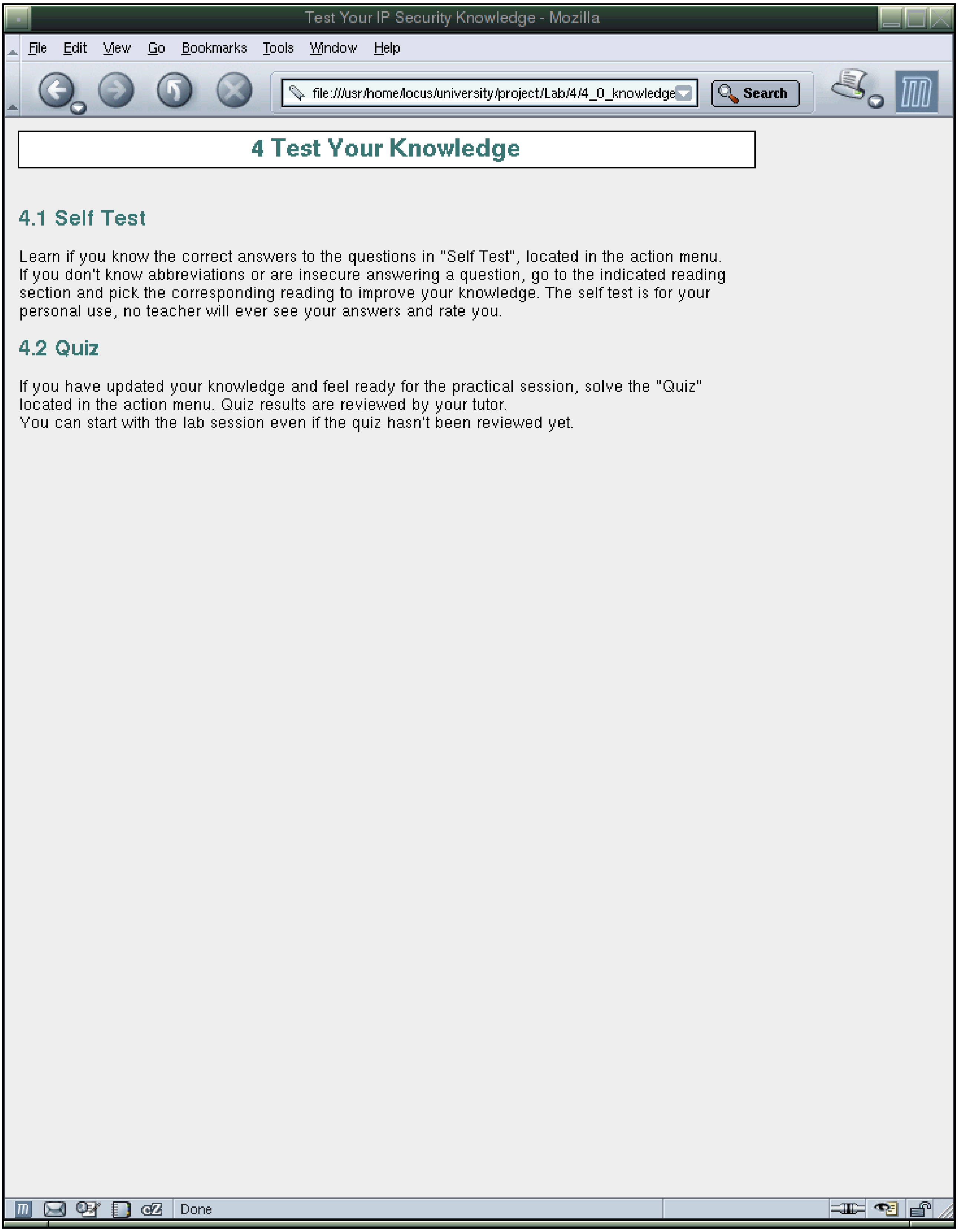
- Cisco 2600/3600 Software Configuration Guide **http://www.cisco.com/univercd/cc/td/doc/product/access/acs_mod/cis3700/sw_conf/37_swcf/index.htm**
- Layer 2 Tunneling Protocol **http://www.cisco.com/warp/public/cc/pd/iosw/prodlit/l2tun_ds.htm**
- IPSec Network Security for Cisco Routers **http://www.cisco.com/univercd/cc/td/doc/product/software/ios113ed/113t/113t_3/ipsec.htm**

IPSec/VPN Related Articles

- IBM VPN Overview **http://www-3.ibm.com/software/network/library/whitepapers/vpn/index.html**
- FreeS/WAN IPSec Documentation **http://www.freeswan.org/freeswan_trees/freeswan-1.95/doc/ipsec.html**
- An IPSec Primer (Université Libre de Bruxelles) **http://www.iihe.ac.be/scimitar/J1000/ipsec**

IPSec RFC's

- Security Architecture for the Internet Protocol (RFC 2401) **http://www.ietf.org/rfc/rfc2401.txt**
- IP Authentication Header (RFC 2402) **http://www.ietf.org/rfc/rfc2402.txt**
- IP Encapsulating Security Payload (ESP) (RFC 2406) **http://www.ietf.org/rfc/rfc2406.txt**
- [RMK+96] Address Allocation for Private Internets **http://www.ietf.org/rfc/rfc1918.txt**



Test Your IP Security Knowledge - Mozilla
File Edit View Go Bookmarks Tools Window Help
file:///usr/home/locus/university/project/Lab/4/4_0_knowledge
Search
Done

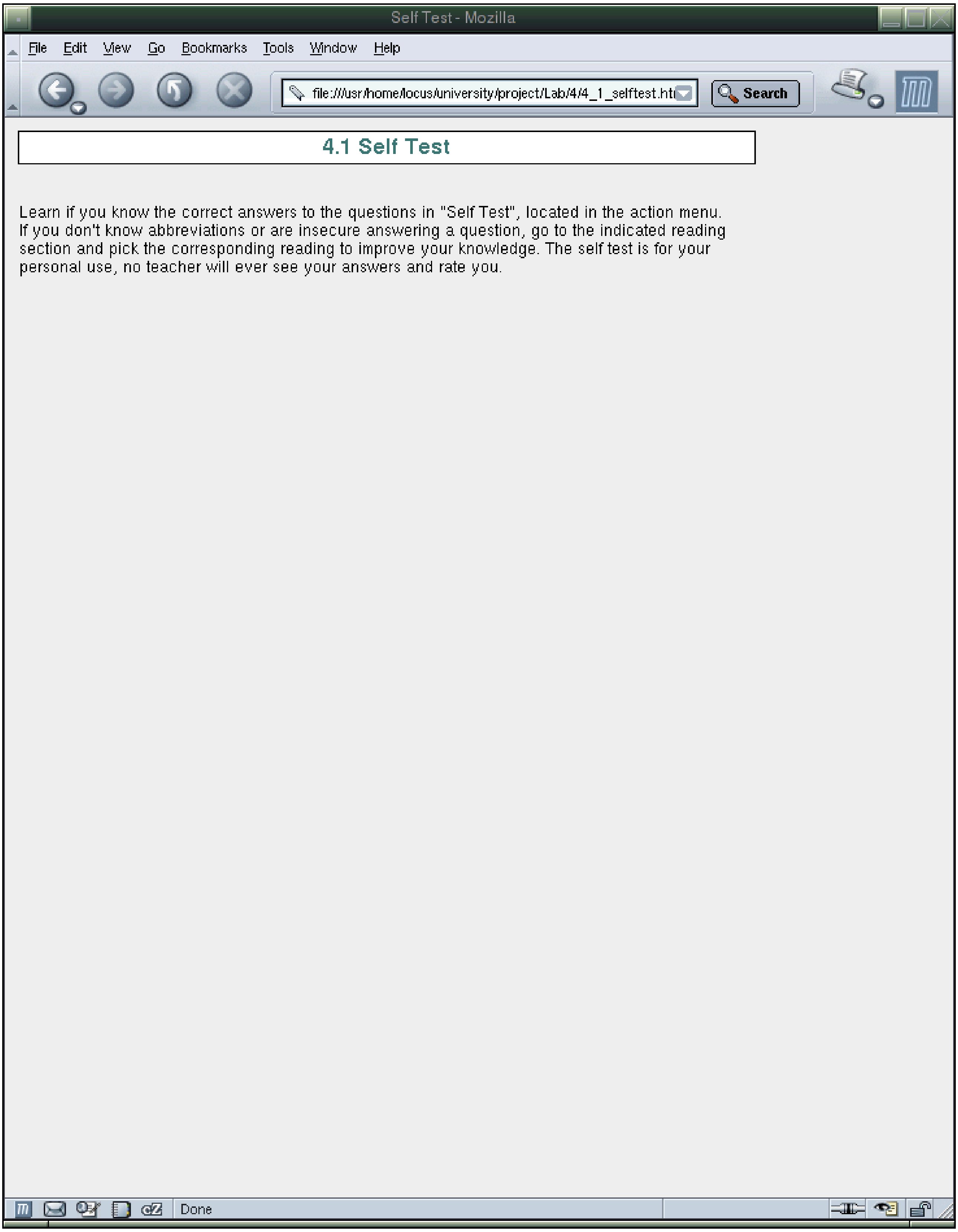
4 Test Your Knowledge

4.1 Self Test

Learn if you know the correct answers to the questions in "Self Test", located in the action menu. If you don't know abbreviations or are insecure answering a question, go to the indicated reading section and pick the corresponding reading to improve your knowledge. The self test is for your personal use, no teacher will ever see your answers and rate you.

4.2 Quiz

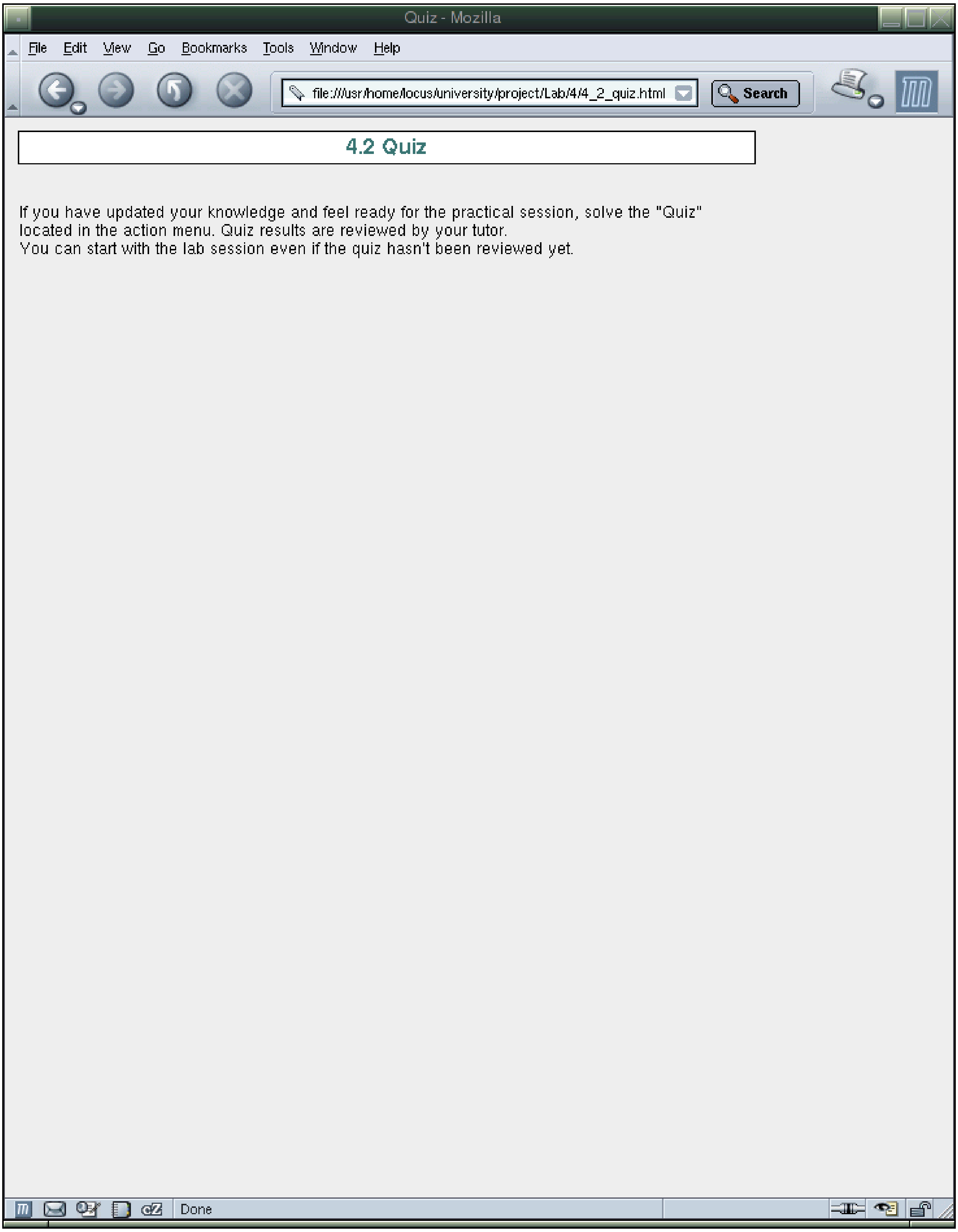
If you have updated your knowledge and feel ready for the practical session, solve the "Quiz" located in the action menu. Quiz results are reviewed by your tutor.
You can start with the lab session even if the quiz hasn't been reviewed yet.



Self Test - Mozilla
File Edit View Go Bookmarks Tools Window Help
file:///usr/home/locus/university/project/Lab/4/4_1_selftest.htı
Search
Done

4.1 Self Test

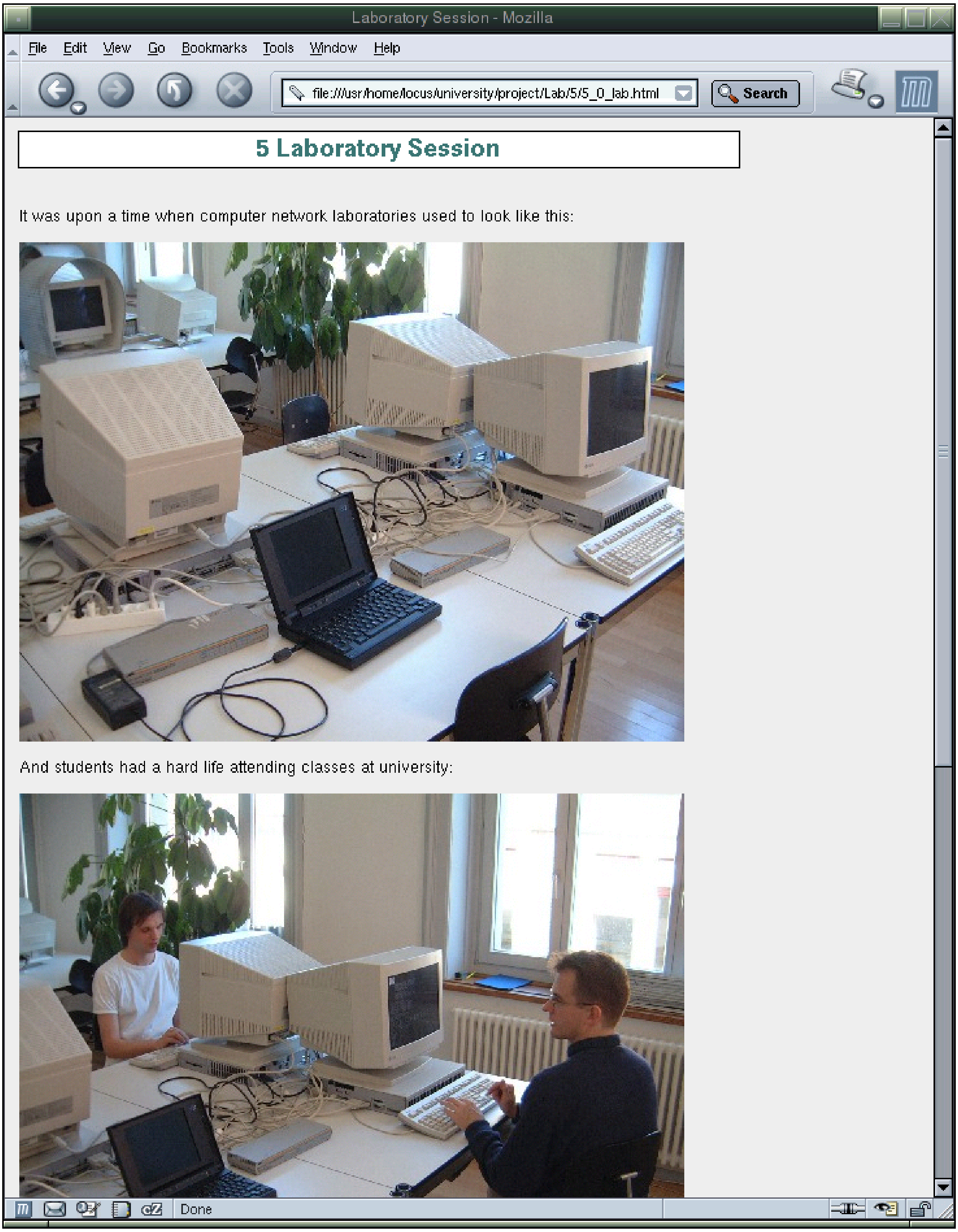
Learn if you know the correct answers to the questions in "Self Test", located in the action menu. If you don't know abbreviations or are insecure answering a question, go to the indicated reading section and pick the corresponding reading to improve your knowledge. The self test is for your personal use, no teacher will ever see your answers and rate you.



Quiz - Mozilla
File Edit View Go Bookmarks Tools Window Help
file:///usr/home/locus/university/project/Lab/4/4_2_quiz.html
Search
Done

4.2 Quiz

If you have updated your knowledge and feel ready for the practical session, solve the "Quiz" located in the action menu. Quiz results are reviewed by your tutor.
You can start with the lab session even if the quiz hasn't been reviewed yet.

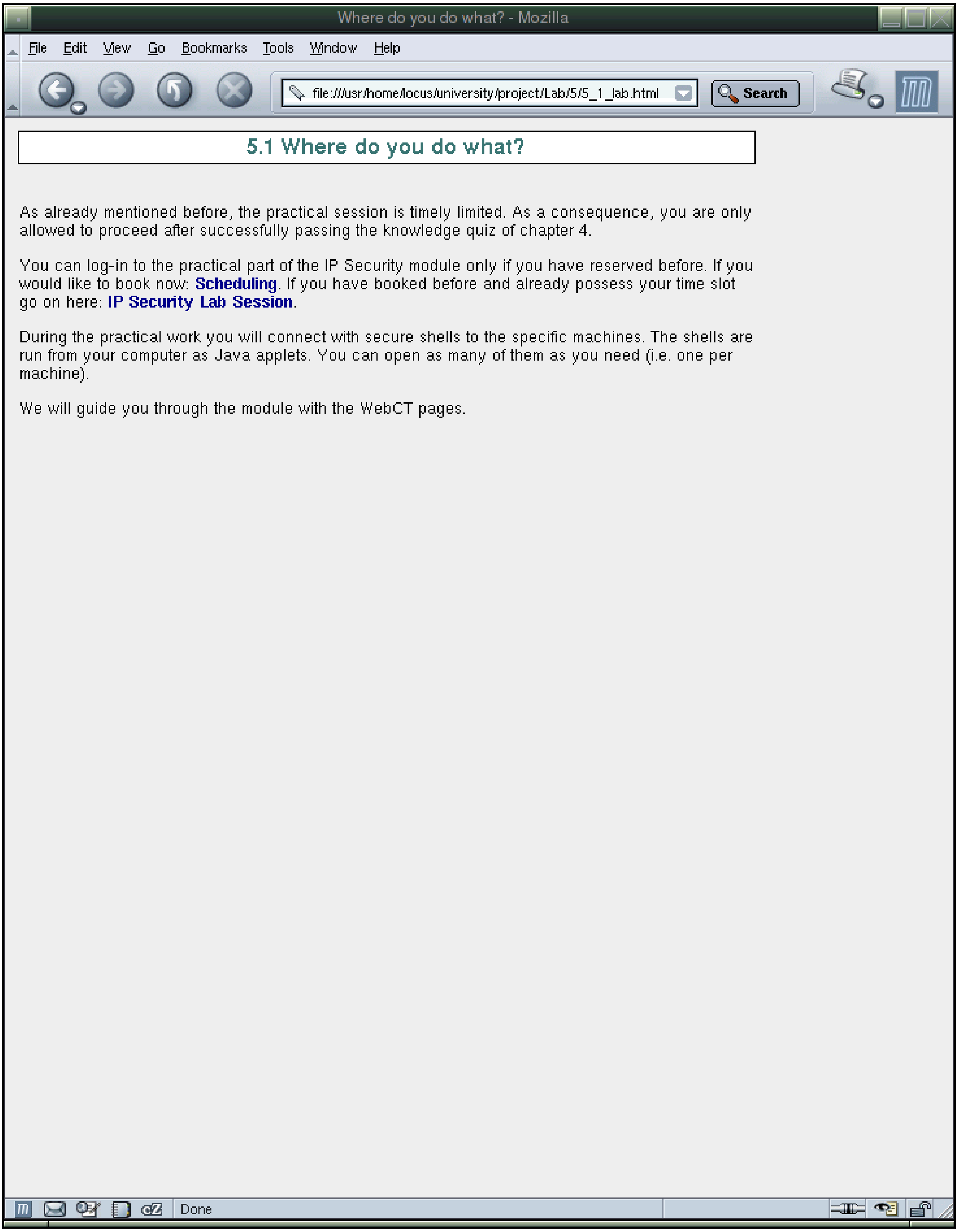


Laboratory Session - Mozilla
File Edit View Go Bookmarks Tools Window Help
file:///usr/home/locus/university/project/Lab/5/5_0_lab.html
Search
Done

5 Laboratory Session

It was upon a time when computer network laboratories used to look like this:

And students had a hard life attending classes at university:


Where do you do what? - Mozilla
File
Edit
View
Go
Bookmarks
Tools
Window
Help
file:///usr/home/locus/university/project/Lab/5/5_1_lab.html
Search
Done

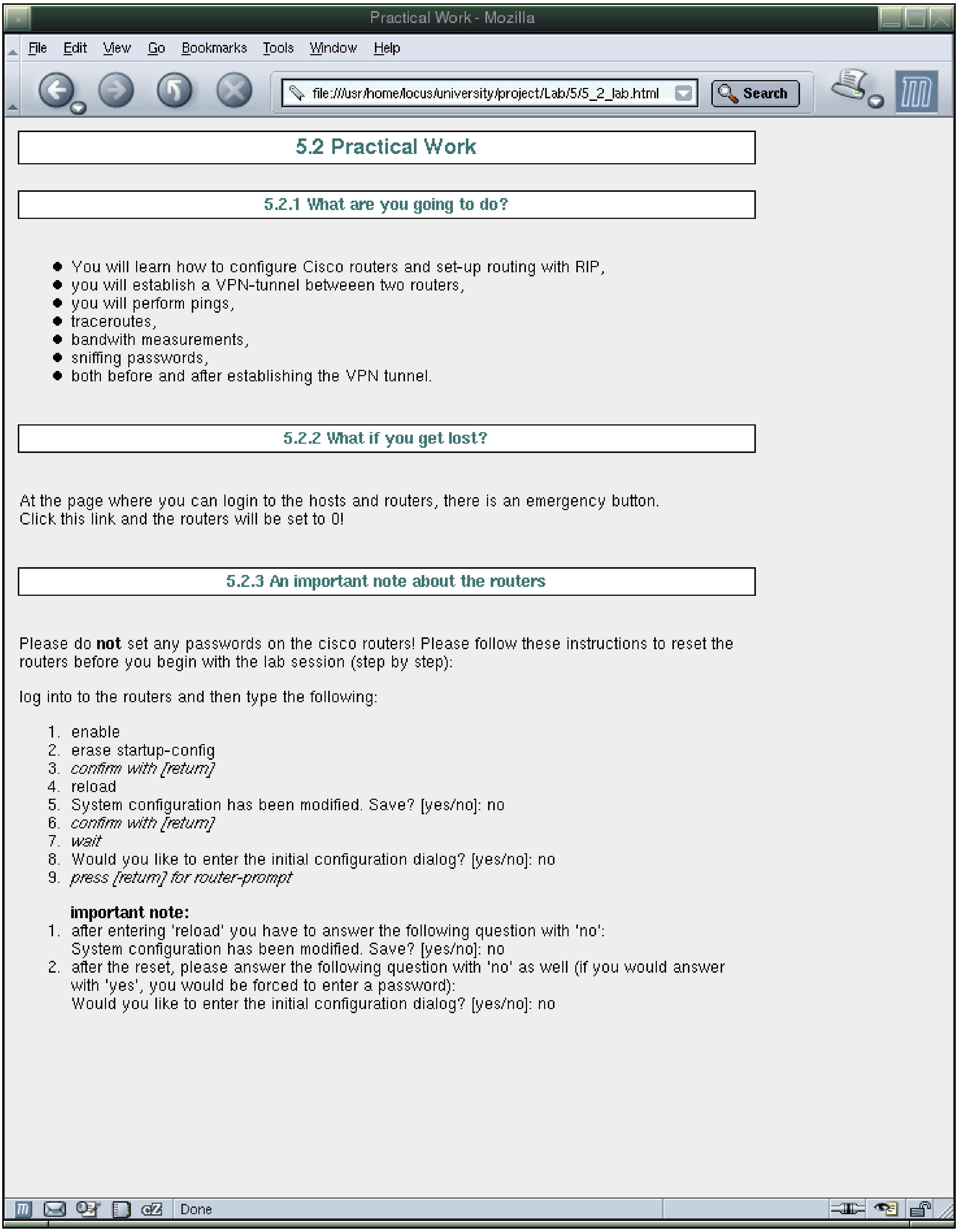
5.1 Where do you do what?

As already mentioned before, the practical session is timely limited. As a consequence, you are only allowed to proceed after successfully passing the knowledge quiz of chapter 4.

You can log-in to the practical part of the IP Security module only if you have reserved before. If you would like to book now: **Scheduling**. If you have booked before and already possess your time slot go on here: **IP Security Lab Session**.

During the practical work you will connect with secure shells to the specific machines. The shells are run from your computer as Java applets. You can open as many of them as you need (i.e. one per machine).

We will guide you through the module with the WebCT pages.


Practical Work - Mozilla
File Edit View Go Bookmarks Tools Window Help
file:///usr/home/locus/university/project/Lab/5/5_2_lab.html
Search
Done

5.2 Practical Work

5.2.1 What are you going to do?

- You will learn how to configure Cisco routers and set-up routing with RIP,
- you will establish a VPN-tunnel betweeen two routers,
- you will perform pings,
- traceroutes,
- bandwith measurements,
- sniffing passwords,
- both before and after establishing the VPN tunnel.

5.2.2 What if you get lost?

At the page where you can login to the hosts and routers, there is an emergency button.
Click this link and the routers will be set to 0!

5.2.3 An important note about the routers

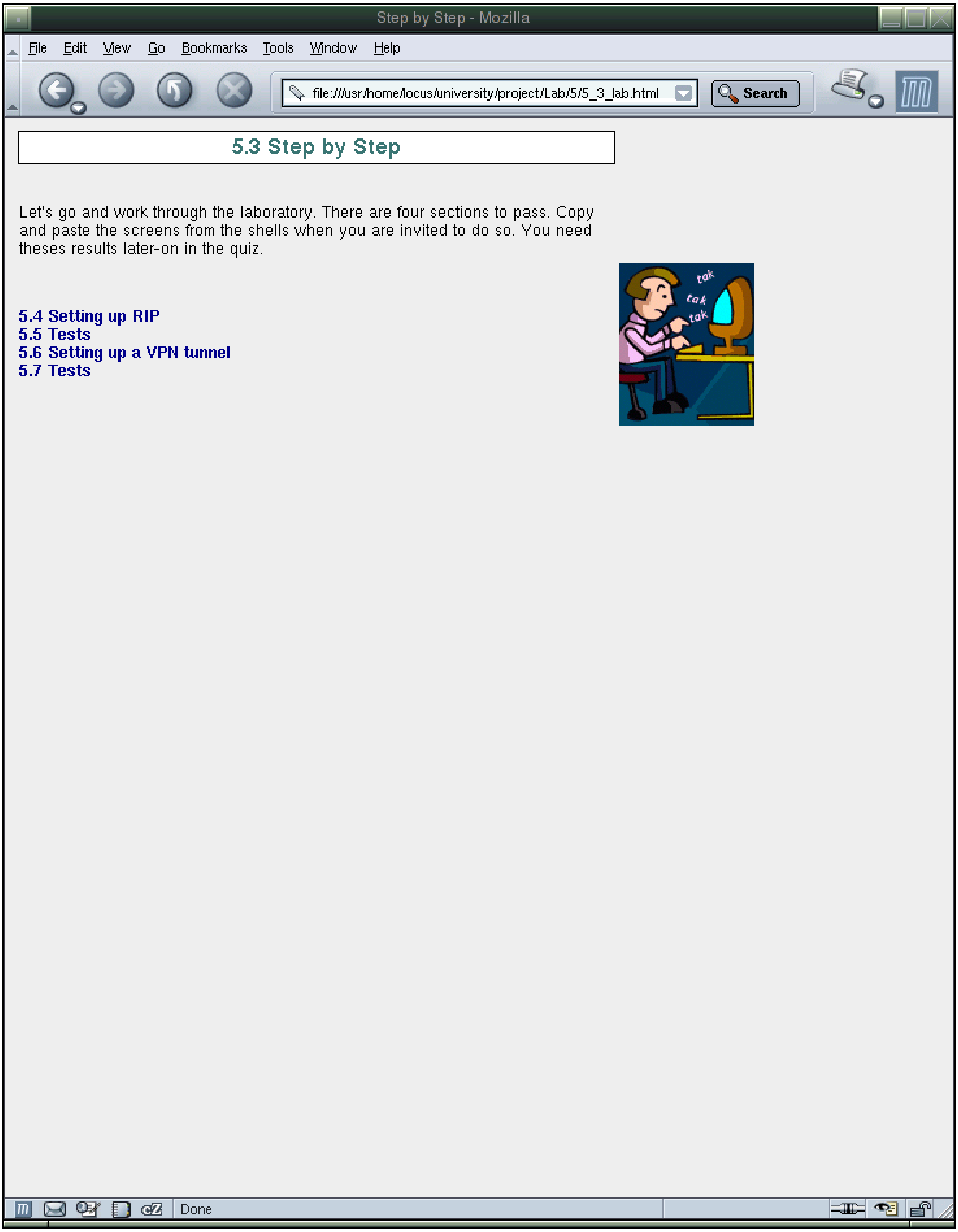
Please do **not** set any passwords on the cisco routers! Please follow these instructions to reset the routers before you begin with the lab session (step by step):

log into to the routers and then type the following:

1. enable
2. erase startup-config
3. *confirm with [return]*
4. reload
5. System configuration has been modified. Save? [yes/no]: no
6. *confirm with [return]*
7. *wait*
8. Would you like to enter the initial configuration dialog? [yes/no]: no
9. *press [return] for router-prompt*

important note:

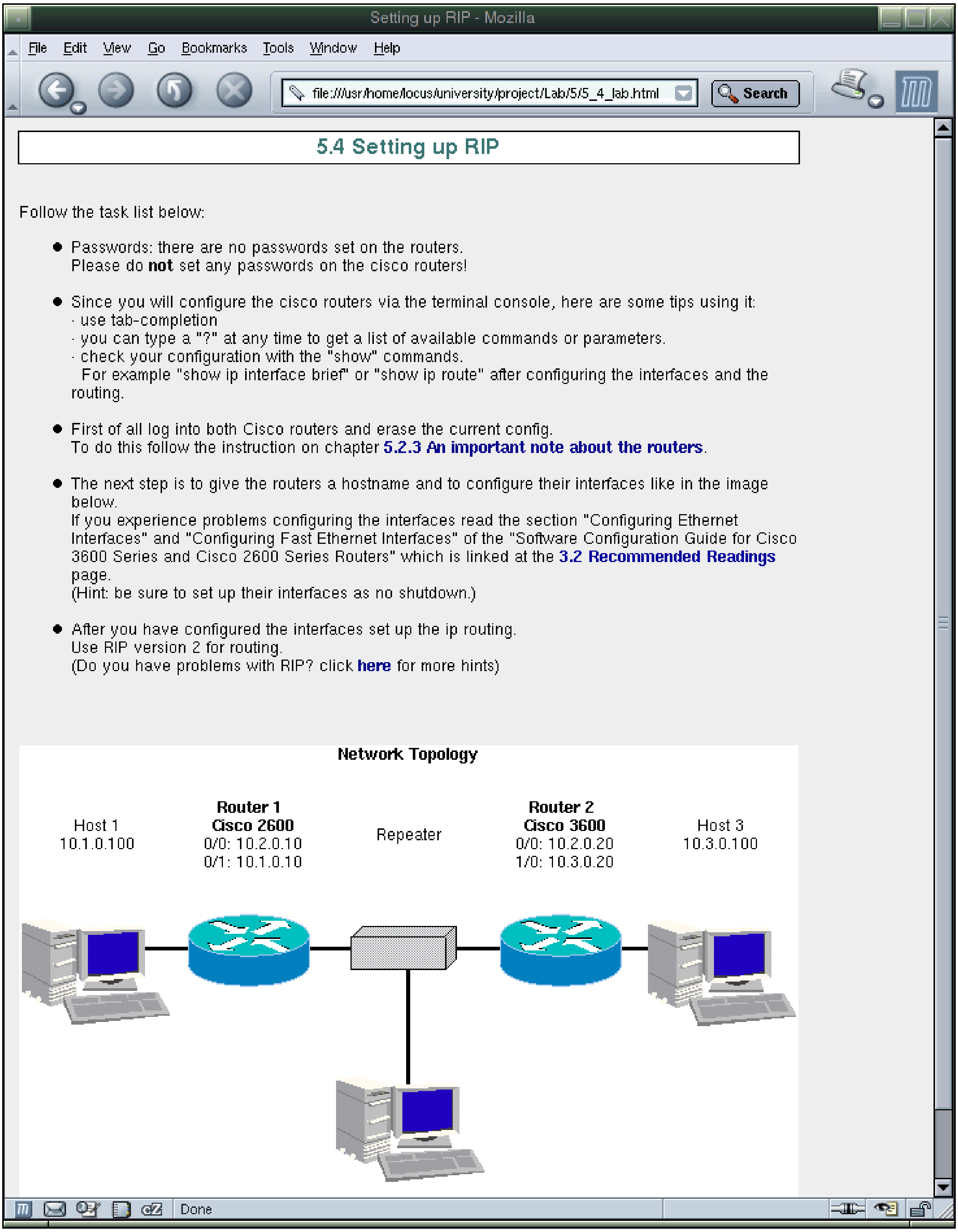
1. after entering 'reload' you have to answer the following question with 'no':
   System configuration has been modified. Save? [yes/no]: no
2. after the reset, please answer the following question with 'no' as well (if you would answer with 'yes', you would be forced to enter a password):
   Would you like to enter the initial configuration dialog? [yes/no]: no


Step by Step - Mozilla
File Edit View Go Bookmarks Tools Window Help
file:///usr/home/locus/university/project/Lab/5/5_3_lab.html
Search
Done

5.3 Step by Step

Let's go and work through the laboratory. There are four sections to pass. Copy and paste the screens from the shells when you are invited to do so. You need theses results later-on in the quiz.

5.4 Setting up RIP
5.5 Tests
5.6 Setting up a VPN tunnel
5.7 Tests



5.4 Setting up RIP

Follow the task list below:

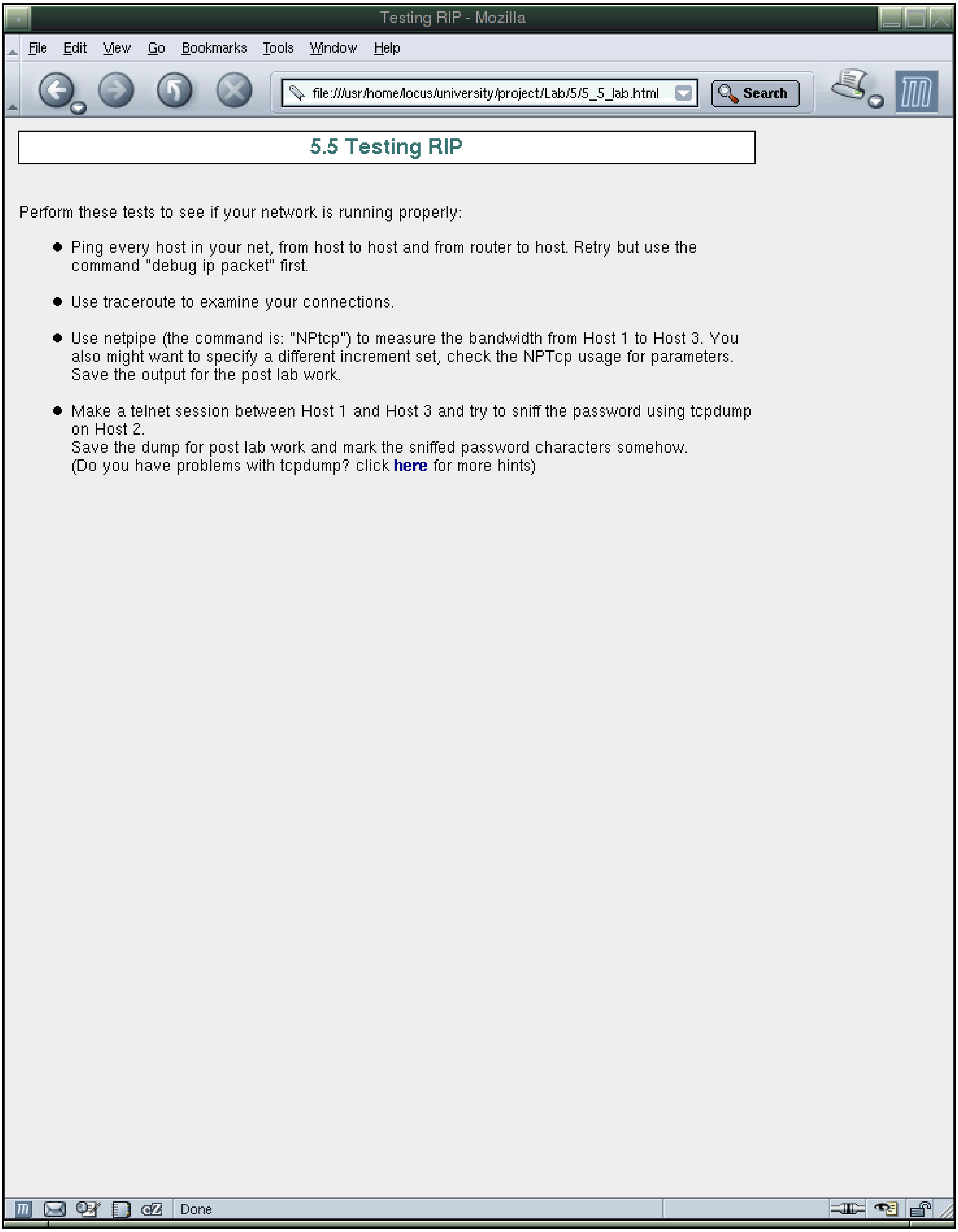
- Passwords: there are no passwords set on the routers.
  Please do **not** set any passwords on the cisco routers!

- Since you will configure the cisco routers via the terminal console, here are some tips using it:
  · use tab-completion
  · you can type a "?" at any time to get a list of available commands or parameters.
  · check your configuration with the "show" commands.
  For example "show ip interface brief" or "show ip route" after configuring the interfaces and the routing.

- First of all log into both Cisco routers and erase the current config.
  To do this follow the instruction on chapter **5.2.3 An important note about the routers**.

- The next step is to give the routers a hostname and to configure their interfaces like in the image below.
  If you experience problems configuring the interfaces read the section "Configuring Ethernet Interfaces" and "Configuring Fast Ethernet Interfaces" of the "Software Configuration Guide for Cisco 3600 Series and Cisco 2600 Series Routers" which is linked at the **3.2 Recommended Readings** page.
  (Hint: be sure to set up their interfaces as no shutdown.)

- After you have configured the interfaces set up the ip routing.
  Use RIP version 2 for routing.
  (Do you have problems with RIP? click **here** for more hints)

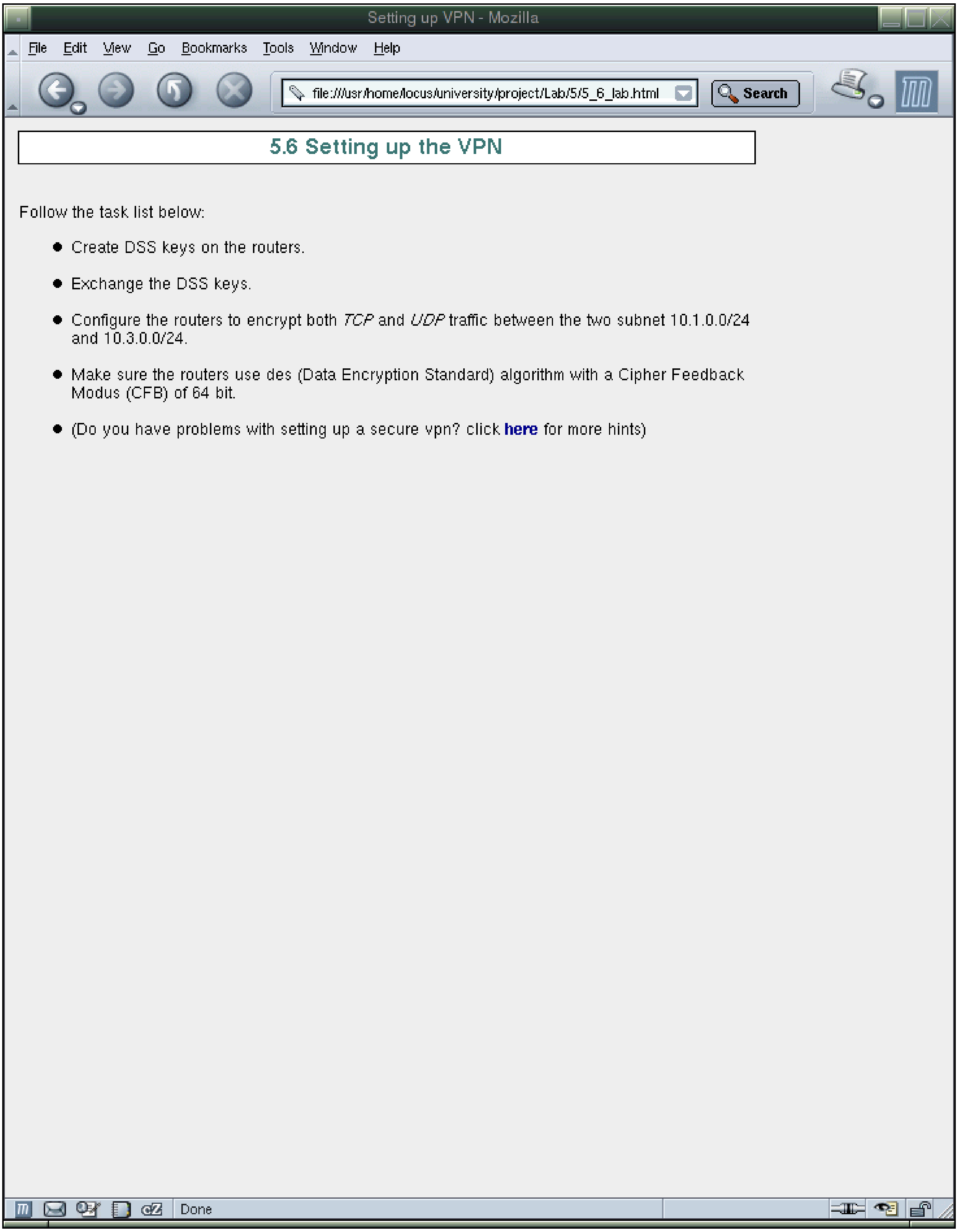


Testing RIP - Mozilla
File Edit View Go Bookmarks Tools Window Help
file:///usr/home/locus/university/project/Lab/5/5_5_lab.html
Search
Done

5.5 Testing RIP

Perform these tests to see if your network is running properly:

- Ping every host in your net, from host to host and from router to host. Retry but use the command "debug ip packet" first.
- Use traceroute to examine your connections.
- Use netpipe (the command is: "NPtcp") to measure the bandwidth from Host 1 to Host 3. You also might want to specify a different increment set, check the NPTcp usage for parameters. Save the output for the post lab work.
- Make a telnet session between Host 1 and Host 3 and try to sniff the password using tcpdump on Host 2.
  Save the dump for post lab work and mark the sniffed password characters somehow.
  (Do you have problems with tcpdump? click **here** for more hints)

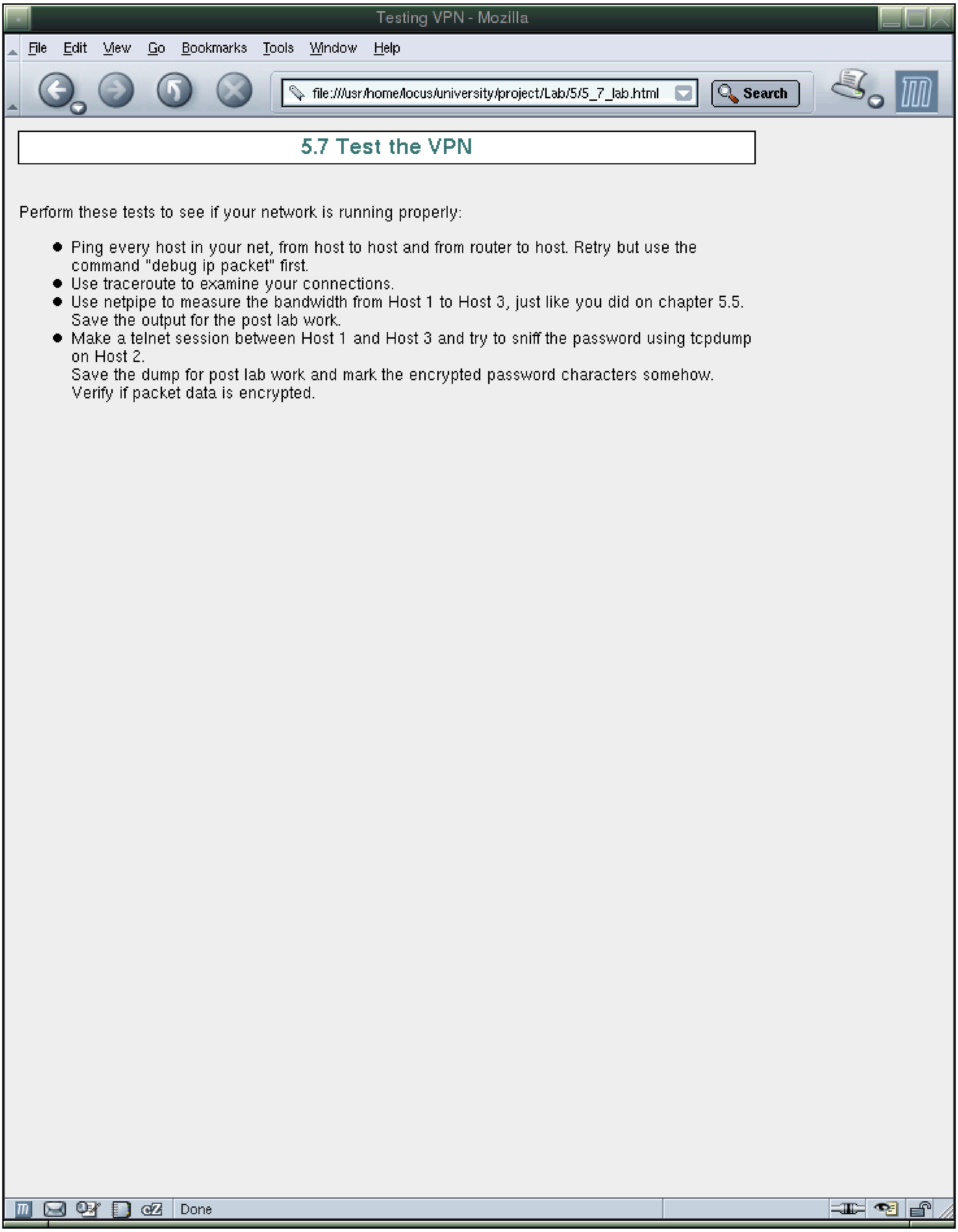


Setting up VPN - Mozilla
File Edit View Go Bookmarks Tools Window Help
file:///usr/home/locus/university/project/Lab/5/5_6_lab.html
Search
Done

5.6 Setting up the VPN

Follow the task list below:

- Create DSS keys on the routers.
- Exchange the DSS keys.
- Configure the routers to encrypt both *TCP* and *UDP* traffic between the two subnet 10.1.0.0/24 and 10.3.0.0/24.
- Make sure the routers use des (Data Encryption Standard) algorithm with a Cipher Feedback Modus (CFB) of 64 bit.
- (Do you have problems with setting up a secure vpn? click **here** for more hints)

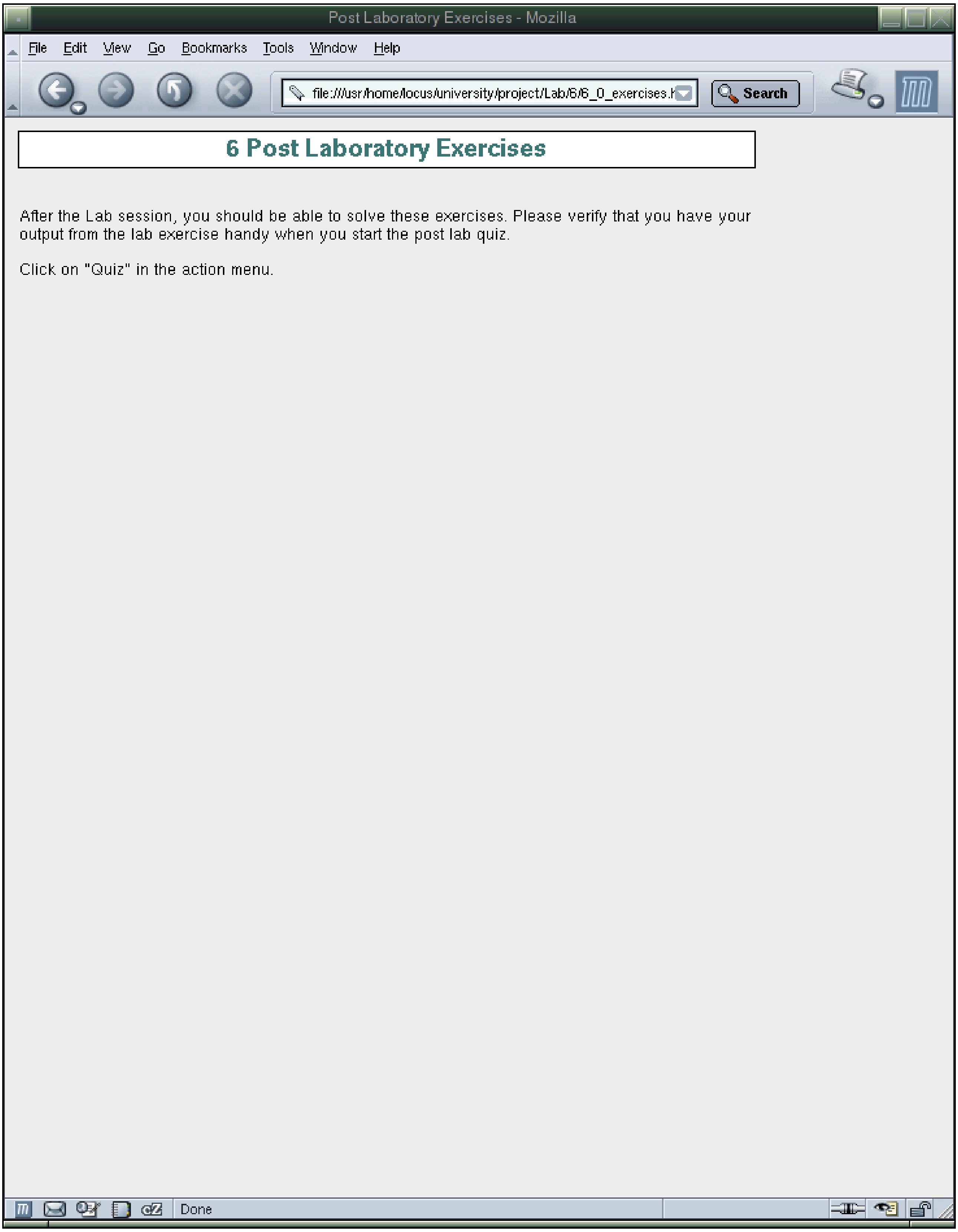


Testing VPN - Mozilla
File Edit View Go Bookmarks Tools Window Help
file:///usr/home/locus/university/project/Lab/5/5_7_lab.html
Search
Done

5.7 Test the VPN

Perform these tests to see if your network is running properly:

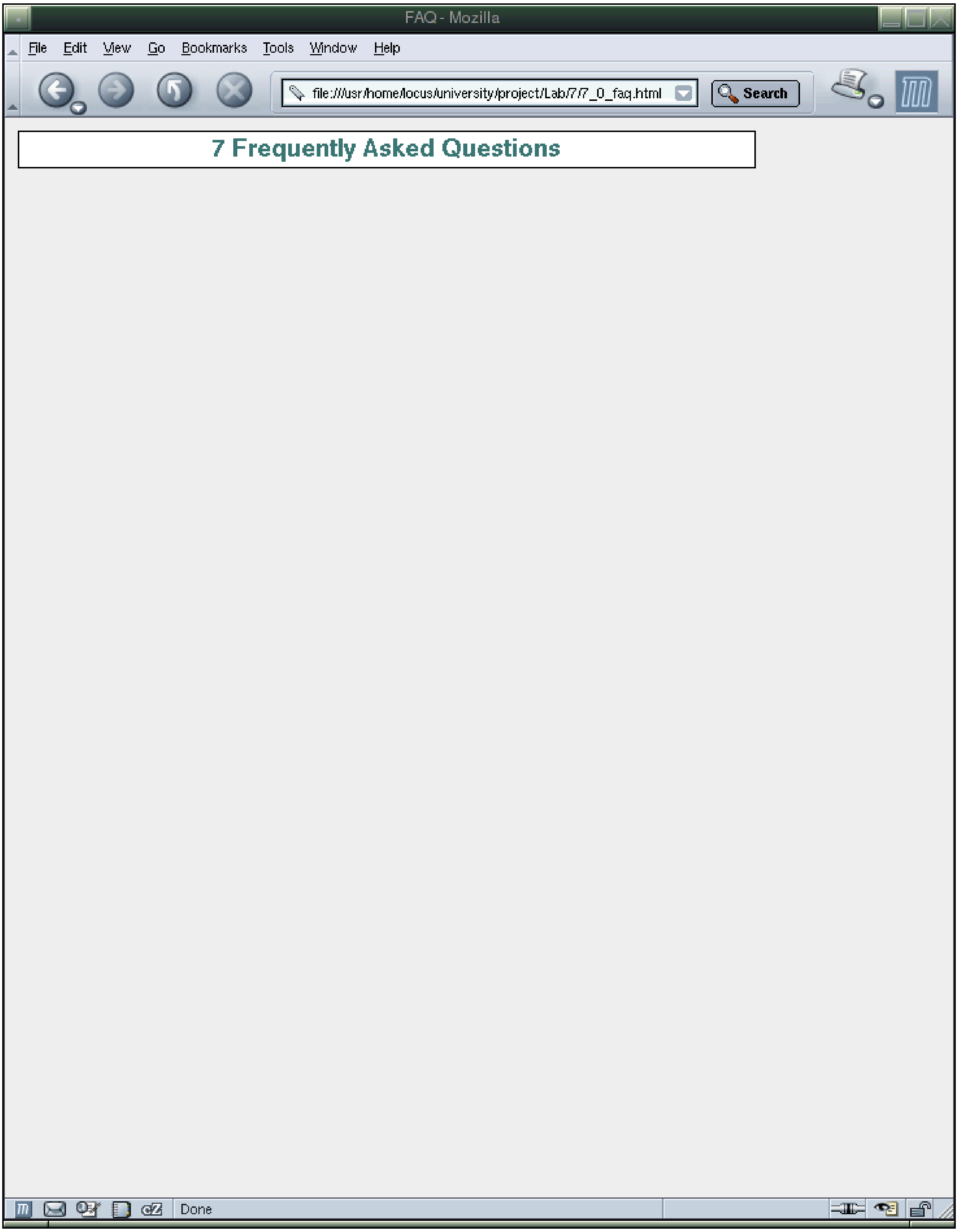
- Ping every host in your net, from host to host and from router to host. Retry but use the command "debug ip packet" first.
- Use traceroute to examine your connections.
- Use netpipe to measure the bandwidth from Host 1 to Host 3, just like you did on chapter 5.5. Save the output for the post lab work.
- Make a telnet session between Host 1 and Host 3 and try to sniff the password using tcpdump on Host 2.
  Save the dump for post lab work and mark the encrypted password characters somehow.
  Verify if packet data is encrypted.


Post Laboratory Exercises - Mozilla
File Edit View Go Bookmarks Tools Window Help
file:///usr/home/locus/university/project/Lab/6/6_0_exercises.h
Search
Done

6 Post Laboratory Exercises

After the Lab session, you should be able to solve these exercises. Please verify that you have your output from the lab exercise handy when you start the post lab quiz.

Click on "Quiz" in the action menu.



7 Frequently Asked Questions