

Part 5

SAFETY

Dr. Małgorzata Langer

Systems & Networks

- Personal computers are more efficient
- Solutions merge different technologies
- Internet is used everywhere
- The number of links grows all the time and the links go beyond state borders without difficulties
- There are more types of user terminals and much greater numbers of them

Internet

- Supports strategic infrastructures – power supply, transport, financing
- Plays a key role in companies' functioning
- Plays a key role in paying governmental services for citizens and companies
- Is an everyday tool in person-to-person communication and messaging

The Safety Culture

- One should concentrate on safety **during the design stage** of IT systems and networks
- The approach should provide for **all users' needs**, the essence of systems, networks and derived services
- **Users should be conscious** of possible safety risks and preventive actions to be taken

OECD GUIDELINES FOR THE SECURITY OF INFORMATION SYSTEMS AND NETWORKS:

TOWARDS A CULTURE OF SECURITY

Governments are expected to promote a culture of security through education, training and awareness-raising activities. Where necessary, governments are encouraged to establish a new policy or amend existing policy with regard to the protection of information systems and networks, according to the **nine** principles

OECD Guidelines

- | | |
|------------------------|-----------------|
| 1. Awareness | implementation |
| 2. Responsibility | 8. Security |
| 3. Response | management |
| 4. Ethics | 9. Reassessment |
| 5. Democracy | |
| 6. Risk assessment | |
| 7. Security design and | |

Awareness

- Participants should be aware of the need for security of information systems and networks and what they can do to enhance security.
- Awareness of the risks and available safeguards is the first line of defence for the security of information systems and networks.

Responsibility

- All participants are responsible for the security of information systems and networks.

Response

- Participants should act in a timely and co-operative manner to prevent, detect and respond to security incidents.

Ethics

- Participants should respect the legitimate interests of others.
- Given the pervasiveness of information systems and networks in our societies, participants need to recognise that their action or inaction may harm others. Ethical conduct is therefore crucial and participants should strive to develop and adopt best practices and to promote conduct that recognises security needs and respects the legitimate interests of others.

Democracy

- The security of information systems and networks should be compatible with essential values of a democratic society.

Risk assessment

- Participants should conduct risk assessments. Risk assessment identifies threats and vulnerabilities and should be sufficiently broad-based to encompass key internal and external factors, such as technology, physical and human factors, policies and third-party services with security implications.

Security design and implementation

- Participants should incorporate security as an essential element of information systems and networks

Security management

- Participants should adopt a comprehensive approach to security management. Security management should be based on risk assessment and should be dynamic, encompassing all levels of participants' activities and all aspects of their operations

Reassessment

- Participants should review and reassess the security of information systems and networks, and make appropriate modifications to security policies, practices, measures and procedures.

LAW

- **1 Oct 2015 - This Recommendation has been replaced by the [Recommendation of the Council on Digital Security Risk Management for Economic and Social Prosperity](#)**

This OECD Recommendation on Digital Security Risk Management for Economic and Social Prosperity and its Companion Document provide guidance for a new generation of national strategies on the management of digital security risk aimed to optimise the economic and social benefits expected from digital openness.

General Principles

1. Awareness, skills and empowerment
2. Responsibility
3. Human rights and fundamental values
4. Co-operation

Operational Principles

- 5. Risk assessment and treatment cycle
- 6. Security measures
- 7. Innovation
- 8. Preparedness and continuity

Telecommunications and Teleinformatics safety in the state system of safety

- The Strategy on National Safety covers telecommunications safety (TiT) as one of the key aspects of **NATIONAL SAFETY**
- In general, TiT relates to many fields, from data safety and methods to communicate, up to the ways of getting data from external sources. It is connected with the phenomenon described as **INFORMATICS WAR**

Informatics War

- Activities based on IT, run during political gridlocks or armed conflicts against 'the other party'
- Exerting influence ahead of the enemy informatics system (data distortion, informational buzz, misinformation...)
- Protecting own systems and data

Safety Assurance

- It is RISK MANAGEMENT, in practice
- One should:
 - indicate potential risks
 - estimate the probability of their occurring
 - estimate potential losses
 - undertake the **REASONABLE** remedial measures

TiT Safety

- The TiT safety, **in details**, is a catalogue of IT issues relating to the possible range of computer networks' protection in the fields of confidentiality, access granting and data integrity.

Operators' opinion 😊

- Operators recommend that these are the sender and the receiver of classified information who should take care on it and keep it in secret. The operator should concentrate on the best services (reliable and fast) and it will help to minimise delays when operations of cipher/decipher are included.

Network Infrastructure Safety

- Safety of basic protocols and network devices in OSI layers
- Safety of wired and radio network infrastructures, and devices (also WiFi, Bluetooth)
- Safety of services (mail, VoIP, IPTV)
- Safety of environment (EMC)

FCAPS – Recommendation ITU-T M3400

- **F**ault Management
- **C**onfiguration Management
- **A**ccounting Management
- **P**erformance Management
- **S**ecurity Management

EMC for Radio Systems

- **Internal EMC** – assuring sufficient safety margin for all system elements – for instance two smartphones, in the same operator's network may be placed very close one to the other and no noise should occur because of that
- **Electromagnetic environment** – one should take care of natural fields that exist near The Globe, and the ones induced by human activities
- **External EMC** – the device should impact environment on as low level as possible and be invulnerable

Technical Possibilities To Obtain and To Modify Messages

- Transmission media:
 - Copper
 - Light fibres
 - Radio
- How 'to fish' the transmitted signal?

Light fibres Advantages

- Light fibres do not emit external electromagnetic field, so one cannot listen to the transmission if he/she is not granted with the physical access. They are very resistant against external electromagnetic noises, BER is lower than 10^{-10} at the highest throughputs, unit damping is low (about 0.20 dB/km for light $1.5\mu\text{m}$).

How to hack into signal?

- The access to light fibres is possible on switching devices, terminals, sometimes also on some routes.
- Some amount of the power can be got through an optical clutch, but to do this one should link off or cut the light fibre:
 - The user may not see that if an automatic switching exists
 - But the operator should see

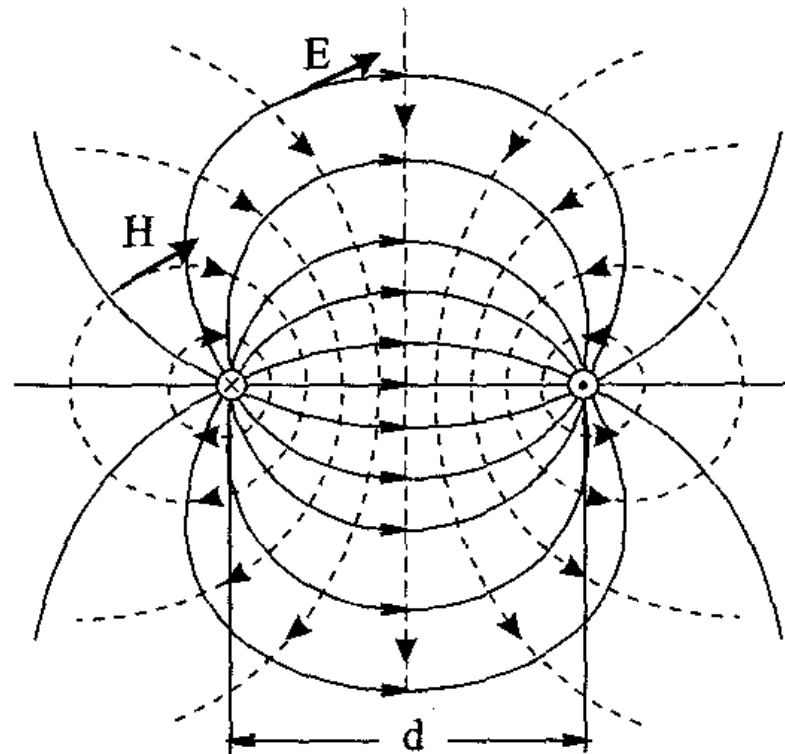
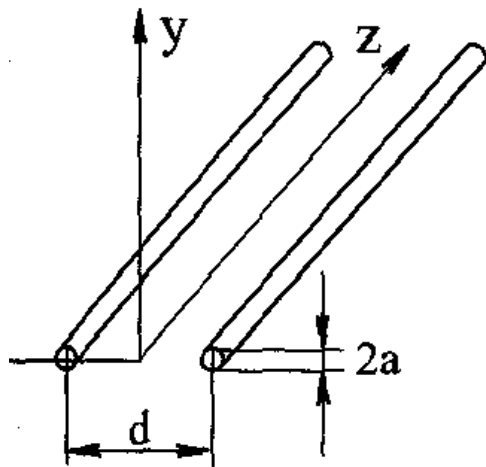
continued.

- Optical clutches of new generation are so sensitive, that 1% power loss is enough to have the signal that can be analysed. So bending the fibre with a small radius is sufficient to hack in
- Each operator monitors the receiving power, but changes in a small range (1 clutch causes the reduction of 0.1 dB to 2 dB only) do not set alarms.

Copper Media

- The analogue signal can be accessed in a simple way
- One can use phenomena of induction, permeating, crosstalk and read the signal without any physical intervention
- Any additional device in the track should be seen by the operator, though the user will see nothing.

Symmetrical Line structure field distribution



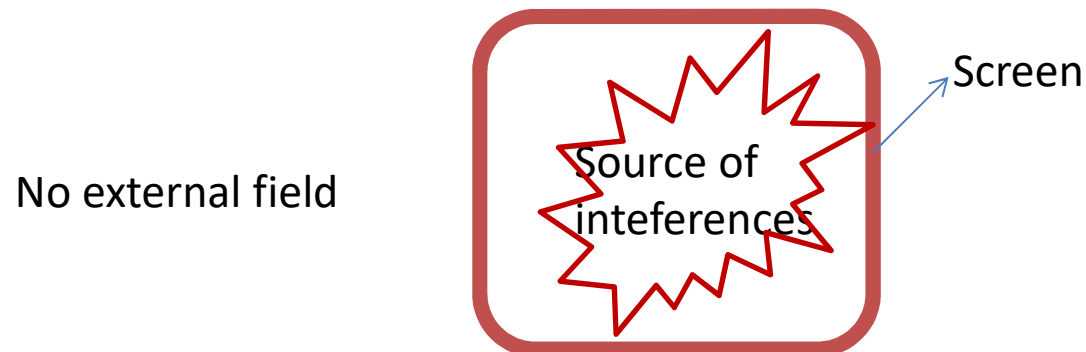
Radio Signal

- It seems the signal can be accessed simply as the medium is accessible;
- The analogue signal without ciphering is vulnerable
- In the new generation systems where one applies modern cipher techniques it is not true and is complicated
- 4G transmission uses different frequencies for one link

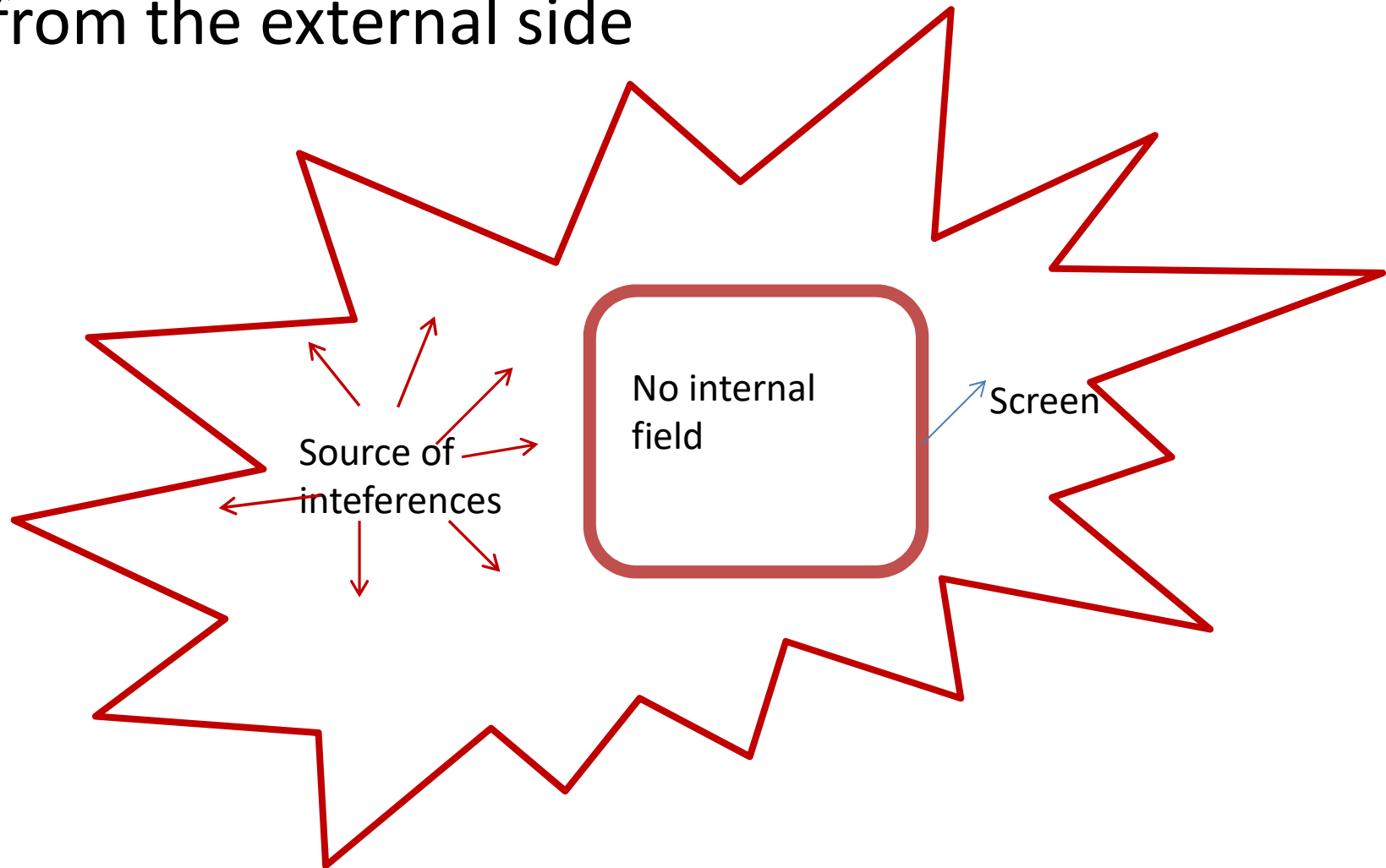
SCREEN

A metal divider placed between two spaces that makes impossible electromagnetic field propagation

The screen may keep the radiation inside the screened area:



Or protect the area against the propagation
from the external side



Threat Categories in Radio (Mobile) Networks

- Unauthorized access to information
 - intercepting sent data
 - using false network devices or pretending to be authorized
 - analysing sent information (for instance to get localisation details)
 - using services in a conflict with their purposes

continued

- Integrity infingement of data (content modification)
- Render difficult to access
 - interfering (jamming)
 - causing network overloads
- Denying to pay
- Using robbed terminals, SIM cards

Protection with devices of UTM and USG types

- The answer is USG (Unified Security Gateway); and UTM (Unified Threat Management) that contain (among others) **Firewall**, to watch the incoming transmission (from Internet), protect against attacks of "Denial of Service" (DoS) type and send message to the Network Manager when the attack attempts occur.
- It is often when Firewall functions are connected with routing and VPN (Virtual Private Network Gateway)

VPN

- VIRTUAL – means, that there is a logical structure, only, destined for a given owner – links' lease holder (PRIVATE), built in a real public network
- VPN nodes are transparent for sent packets, it is a direct logical link between two terminals (clients), that works like a physical private link
- This is the ideal solution for tele-work

Tunneling Protocols

- Point-To-Point-Tunneling-Protocol (**PPTP**), proposed by Microsoft, used with MS Windows, later also with other OSes
- One may transmit TCP/IP packets through another type network
- PPTP may be used to link different physical networks

PPTP – continued

- It does not cover authorisation and/or ciphering (but there are some solutions with these mechanisms).
- PPTP works in the 2nd layer (Data Link). It may be used with Point to Point Encryption (MPPE) Microsoft protocol.
- IT IS A PART OF Windows OS; (other versions are built in Android (phones), also MAC; one can install it to Linux

PPTP, continued

- It has been hacked many times, especially in basic versions
- Also the version L2TP (Layer 2 Tunneling Protocol), used in MS Windows was not resistant against blocking by some firewalls and NAT (*Network Address Translation*) programs

IPsec

- Internet Protocol Security – It is a set of protocols to start and to apply safe links and to exchange ciphered keys.
- VPN based on IPsec consists of at least 2 channels: one channel, with UDP protocol – for key exchange and the others – data packets with ESP (Encapsulating Security Payload)

IPsec – continued

- The origin IP packet is ciphered, encapsulated (it obtains IPsec overhead) and sent to the network
- Symmetrical keys are the fastest ones, but the asymmetrical cryptography secures much better
- **IKE** (Internet Key Exchange) Protocol was designed to distribute and to authenticate keys

Ipssec Overhead

- SPI (Security Parameters Index) - the constant for the transmission in a given channel, generated randomly during the channel creation
- Successive Number – drawn and incremented by 1 with each packet

In Radio Mobile Network

- Since Rel 5 (in UMTS) one has recommended applying IPSec not only for signaling but also for transmitted packets.

SSL (Secure Sockets Layer) Protocol

- SSL is the Transport Layer protocol (above TCP/IP and below Application) in OSI. It consists of two parts: *handshake protocol* and *record protocol*
- During linking there is an exchange of references (authentication) and then safety parameters' negotiation

SSL assures:

- **Authentication** (Verifying servers or a server and a client on the both ends)
- **Confidentiality** (Ciphering according to Master Secret/ shared secret)
- **Integrity** – preclusion for changing message content

Master Secret

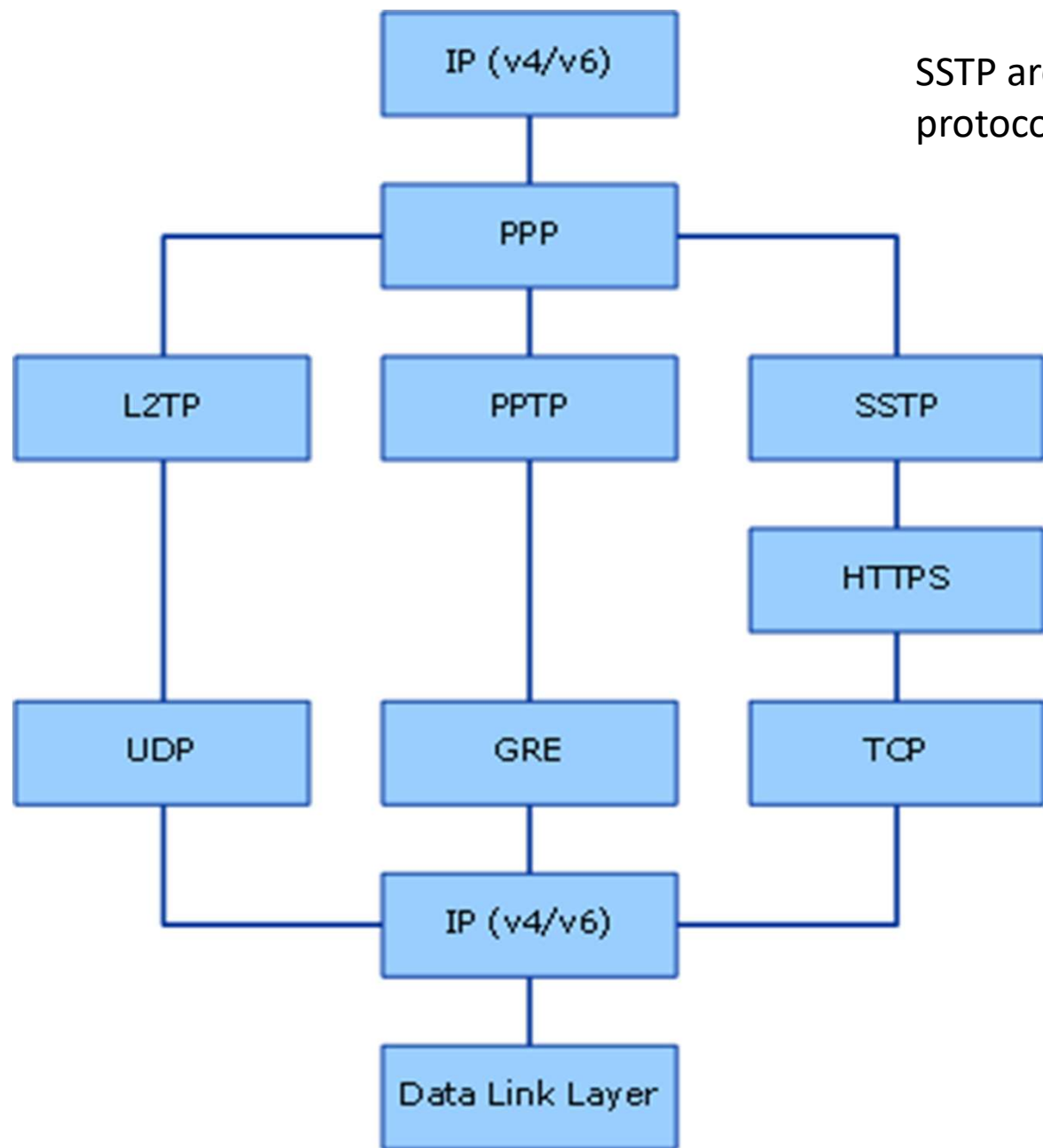
- 49-bit secret control string, ciphered with the server's public key, used to cipher all later communication.
- But the public cryptography key may be used to create „shared secrets“, such a transmission is ciphered in a way that only two parties know

Integrity in SSL

- The block with ciphered data is secured by wrapping (*wrapper*)
- SSL became the basic protocol for many applications (tele-work, e-commerce, radio access devices, web services and others)

SSTP Protocol

- Since Vista, Microsoft has introduced SSTP (Secure Socket Tunneling Protocol)
- It is based on SSL, but supports tunnelling, only



SSTP architecture on the protocols level

PPP

- PPP – Point-to-Point-Protocol (encapsulate method, Link Control Protocol – to manage link modes: opened, maintained, closed, max packet, and so on, Network Control Protocols to process addresses, masks, DNS servers' list)
- This is the set of more than 25 protocols

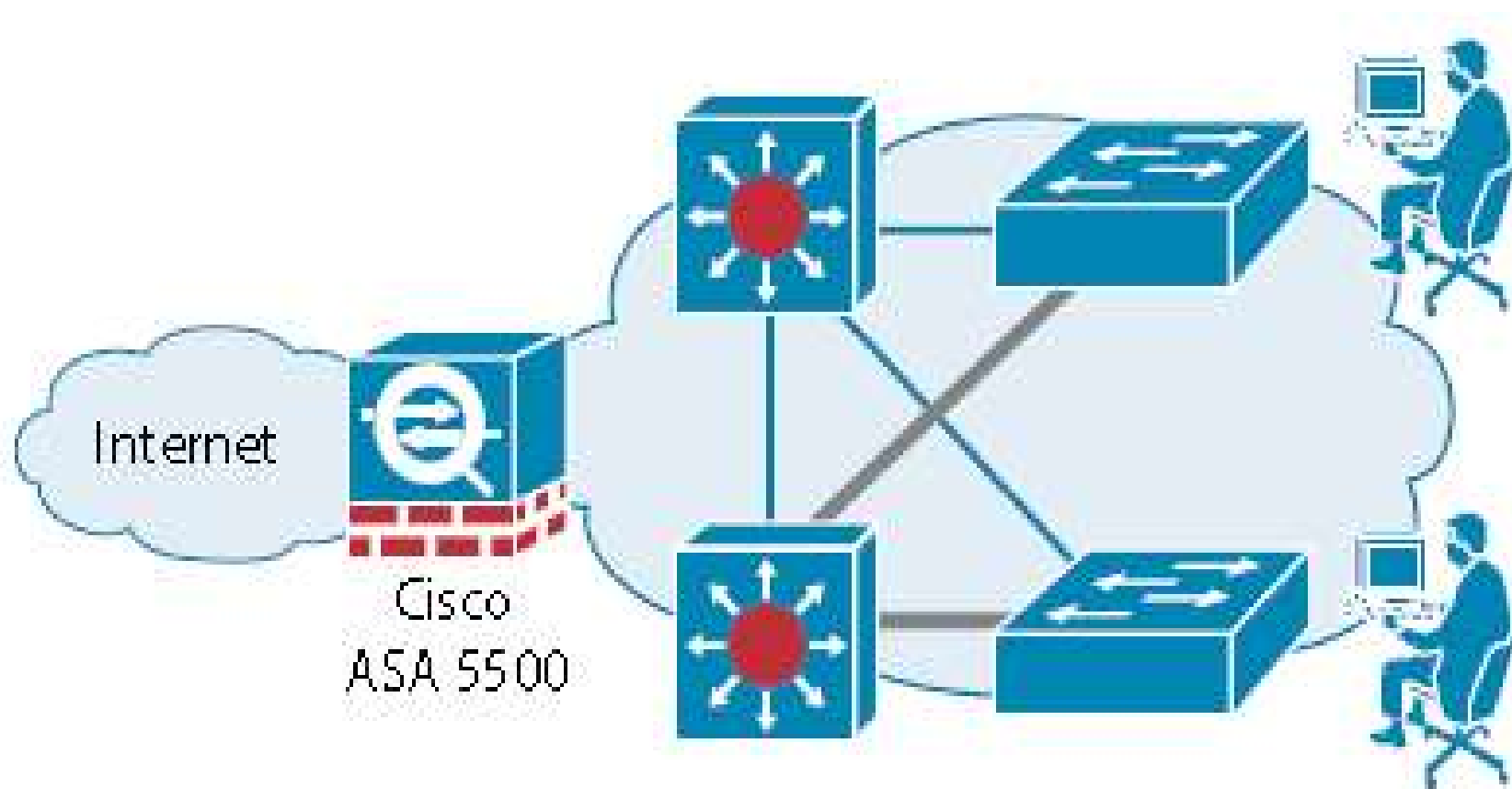
HTTPS

- **HTTPS** - HyperText Transfer Protocol Secure – the ciphered version of HTTP protocol
- The first step is: the exchange of SSL keys, then HTTP is called
- HTTP makes possible www (web) viewing; sends demands to give access to www documents, sends info that the web link was 'clicked', sends information from web forms
- It does not keep any data (there are other mechanisms do that)

GRE Protocol

- GRE - Generic Route Encapsulation . GRE carries data between two end points of the tunnel (Cisco firm protocol)
- When the PPTP control session is established, GRE Protocol is used to seal the encapsulation of data or load

The example (CISCO)



Intermediate server (PROXY)

- Anonymity in the network?
- There is a special software to connect to internet through intermediate server
- Such servers accelerate loading processes as they keep in the memory many www pages

Types of Proxy

- **high anonymous** – The receiving server has no information that we use Proxy server AND HAS NOT our IP
- **anonymous** - The receiving server has information that we use Proxy server AND HAS NOT our IP
- **transparent** – our IP is explicit; we load webs faster

Other advantages of Proxy

- Blocking dangerous scripts
- Blocking unwanted advertisements
- Possibility of cookies' management
- So, some kind of increasing the user safety
- BUT: many webs do not allow for the access of proxy servers (anonymity)

Access Control List - ACL

- ACL allows the router to undertake the decision: to allow the given packet for in/outgoing basing on the criteria. The list is configured in a global mode (IP numbers), but used on one, given interface; **PACKETS ARE FILTERED**
- The filtration starts from the top of the list. When a hit occurs the planned action is made and the further processing of ACL is stopped for the packet.

ACL - standard

- Based on IP numbers (**only**). There are two possibilities:

PERMIT

or

DENY

- The standard says, that if no hit is met, the last line (for the others) should be DENY

Other functions of ACL

- Limitation of upgrades sent by routing protocols
- Defining affiliations of packets to successive queues (QoS mechanisms)
- Controlling the access to ssh lines
- etc.

ACL – widened

- One may consider not only IP, but also the source or the purpose (but then one must go higher than the Transport Layer is)
- Examples: Allow or don't allow for telnet, FTP, interactive web viewing...

Access Lists (ACL)

- One may have many lists on one router. Every list must have its unique number or name
- The range for **standard lists**:
1-99 and 1300 – 1399
- For **widened lists**:
100-199 and 2000 - 2699

List Numbers for other systems and protocols - examples

- RouterA(config)#**access-list ?**

<1-99>	IP standard access list
<100-199>	IP extended access list
<200-299>	Protocol type-code access list
<300-399>	DECnet access list
<400-499>	XNS standard access list
<500-599>	XNS extended access list
<600-699>	Appletalk access list
<700-799>	48-bit MAC address access list
<800-899>	IPX standard access list
<900-999>	IPX extended access list
<1000-1099>	IPX SAP access list
<1100-1199>	Extended 48-bit MAC address access list
<1200-1299>	IPX summary address access list

ACL – continued

- Only one list may exist for the interface, for the protocol or for the direction (for example one ACL for incoming IPs and one ACL for outgoing ones) The list must be installed
- Every list must have at least one 'permit', if not, it would be total closing the interface. (as ;default; all no mentioned IPs are dropped)
- If the Access List is empty – the whole traffic goes through

ACL standard

- „reach” IP protocol content, only (Network Layer)
- IP functions:
 - Source routing
 - Routing Operations
 - Loose and strict routing
 - Route-Recording Option)
 - Timestamp Option – in milliseconds, (Greenwich time)
 - ICMP (Internet Control Message Protocol)