CII-3E3
Cybersecurity

NETWORKING AND COMMUNICATIONS

Outline Today

- What is the Internet?
- Is your private information really private?
- Why we need standards on the Internet?

WHAT IS THE INTERNET?

The Internet

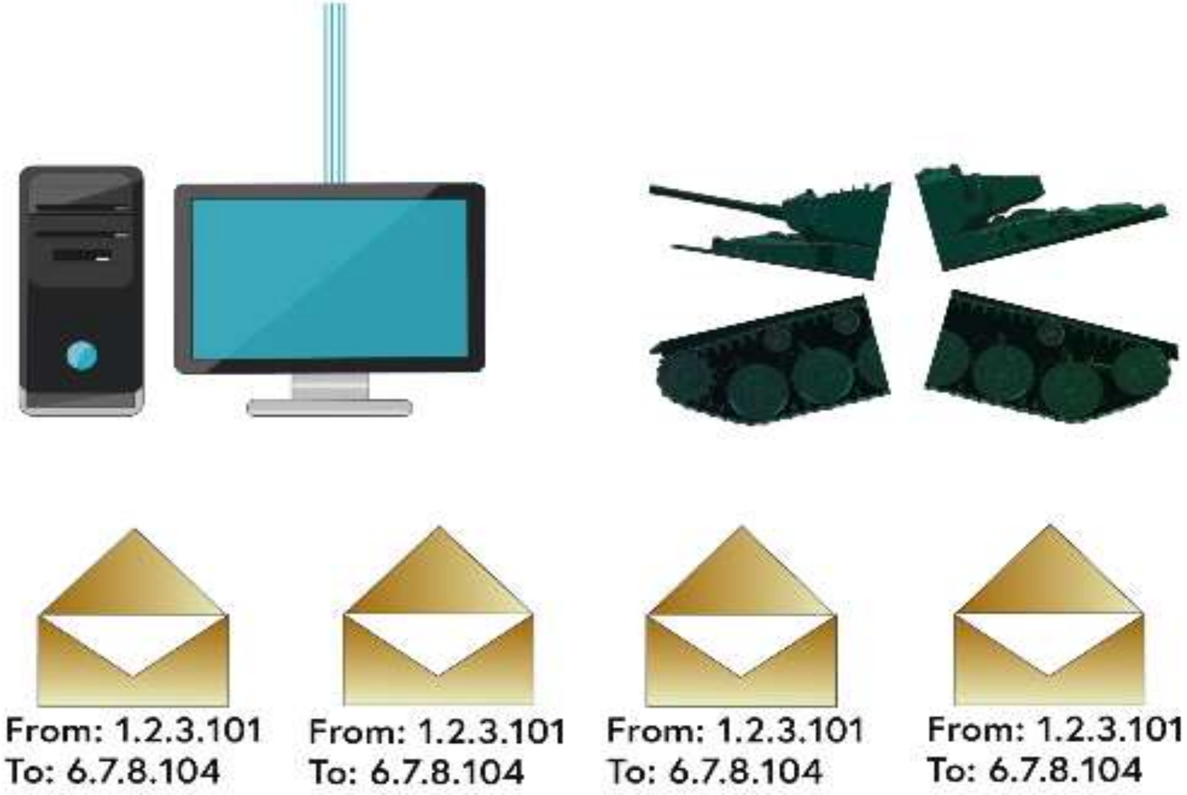
- not a single entity with a single owner
- comprises a hierarchy of individual networks that have been connected to one another
- Definition : a network of networks

Key factors in the Internet design

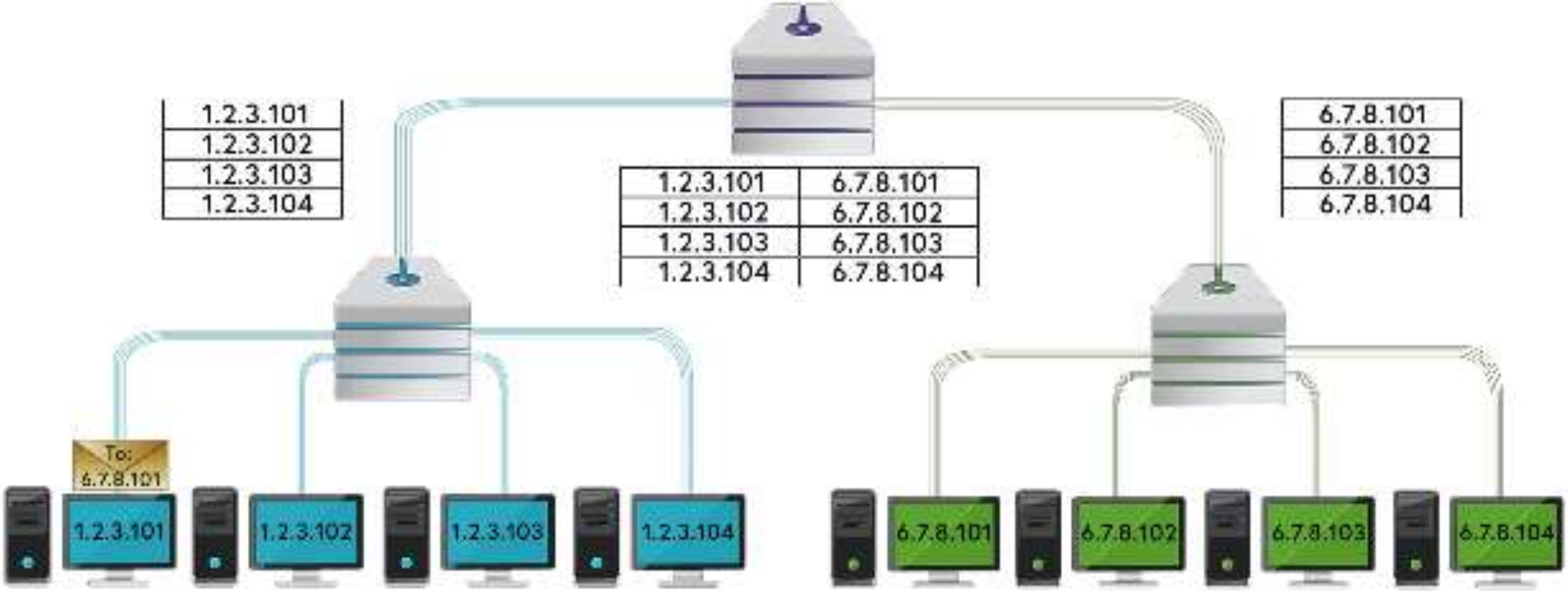
- The network would not have a central controlling computer.
  - Each computer on the network would be assumed to have the same authority as every other computer
- The network should be able to deliver information between any two computers on the network even if some of the machines in the network had failed.

How data moves around the Internet (1)

- Packet is shown with destination address 6.7.8.104



How data moves around the Internet (2)



1.2.3.101
1.2.3.102
1.2.3.103
1.2.3.104

1.2.3.101	6.7.8.101
1.2.3.102	6.7.8.102
1.2.3.103	6.7.8.103
1.2.3.104	6.7.8.104

6.7.8.101
6.7.8.102
6.7.8.103
6.7.8.104

Introducing the datagram

- When data, such as a picture, movie or a document is sent over the internet, it is not sent as a single chunk
- Instead it is split up into small, uniformly sized blocks called ‘datagrams’, also sometimes called ‘packets’.
- One envelope (the ‘header’) and its contents correspond to a single datagram.

Header

- Header contains the sender and recipient’s addresses, a unique number, a date stamp and some error correction information
- The contents (called the ‘payload’) contains the actual information being delivered.

Wireless networks

- Early computer networks depended on wires
- Now → wireless (radio) connections
- Wi-fi enables devices such as computers and printers to be connected together wirelessly to form a local area network (LAN)

Wi-fi

- ‘wi-fi’ refers in particular to wireless local area networking technology that is compliant with a particular family of standards maintained by the Institute of Electrical and Electronics Engineers (IEEE) and called the 802.11 family.
- Different variants of this standard on wireless routers, for example 802.11b, 802.11g and 802.11n.

Service set identifier (or SSID)

- The ‘service set’ → the set of wireless devices to be served by a particular wireless LAN
- SSID allows the nodes on a wireless LAN to distinguish themselves from nodes on other wireless LANs that may be operating in the same physical space.

IS YOUR PRIVATE INFORMATION REALLY PRIVATE?

Network security challenges

- Programmed with strategies to overcome problems such as congestion or the failure of a part of the network.
  - re-routing datagrams via any alternative direction
- Routers will most probably not belong to either the sender or the recipient, but a third party
  - datagrams can be copied, and their security compromised → packet sniffing

Encryption in wireless networking

- Ensuring that the eavesdropper is not able to convert these signals into the original message → confidentiality
- Malicious users could interpose themselves between a sender and a receiver and modify the messages or even destroy (MITM)

→ Integrity

Encryption in wireless networking (2)

- Attacker could transmit lots of random data on the frequency being used by the wireless network, congesting the network and thus preventing other users from sending data (DoS attack)

→ Availability

Using wireless networking securely

Encryption, ensure:

1. Confidentiality – When a message is encrypted using a particular key, it can only be decrypted to recover the original information if the same key is used.
2. Integrity – Encryption can prevent messages from being modified without the receiver's knowledge.
3. Authentication – Encryption can contribute to the process of proving the identities of the sender and receiver.

Encryption in wi-fi

- Using a key known only to the nodes in the wireless network
- Wired Equivalent Privacy (WEP) → confidentiality comparable to that of a wired network.
- Wi-fi Protected Access 2 (WPA2) →

  a more secure key to encrypt the transmitted data.

  (default configuration : compliant with the 802.11 standard)

WHY WE NEED STANDARDS ON THE INTERNET?

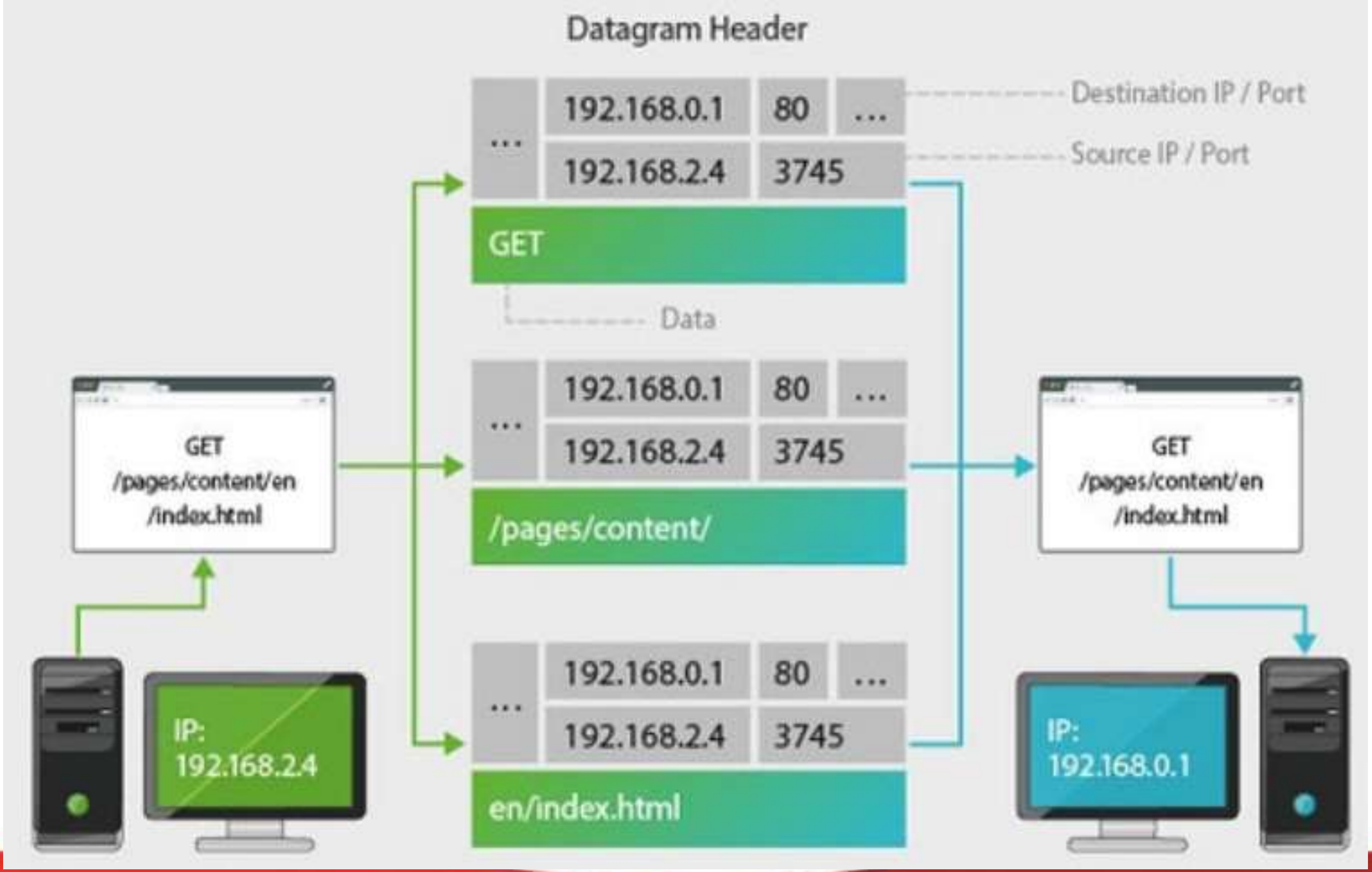
Introducing the TCP/IP protocols

- Communications protocols : standards that allow different networks and differing communications equipment to talk to one another are formalised in digital rules
- Internet :
  - Transmission Control Protocol (TCP),
  - Internet Protocol (IP).

TCP

- Responsible for ensuring data can be sent reliably over the internet (but relatively slow).
- Port represent specific protocols such as
  - port 80 representing the well-known port of HTTP.
  - port 20 and 21 – File Transfer Protocol (FTP) for sending and receiving files (port 20) and control (port 21)
  - port 22 – Secure Shell (SSH) for secure logins to computers
  - port 25 – Simple Mail Transfer Protocol (SMTP) for sending email

TCP(2)


Datagram Header
...
192.168.0.1
80
...
192.168.2.4
3745
Destination IP / Port
Source IP / Port
GET
Data
GET
/pages/content/en
/index.html
...
192.168.0.1
80
...
192.168.2.4
3745
/pages/content/
GET
/pages/content/en
/index.html
IP:
192.168.2.4
...
192.168.0.1
80
...
192.168.2.4
3745
en/index.html
IP:
192.168.0.1

UDP (User Datagram Protocol)

- Applications where timeliness is more important than absolute accuracy.
- less reliable, but faster
  - streaming media, video games and video conferencing
- Receiving an email → the whole message to arrive with no gaps
- Streaming a TV programme → it doesn’t greatly matter if a few datagrams get lost.

The Internet Protocol (IP)

- TCP is not responsible for sending and receiving information → IP
- IP is only concerned with moving data, it doesn't actually check that data actually arrives (that's handled by TCP).

The Internet Protocol (IP) (2)

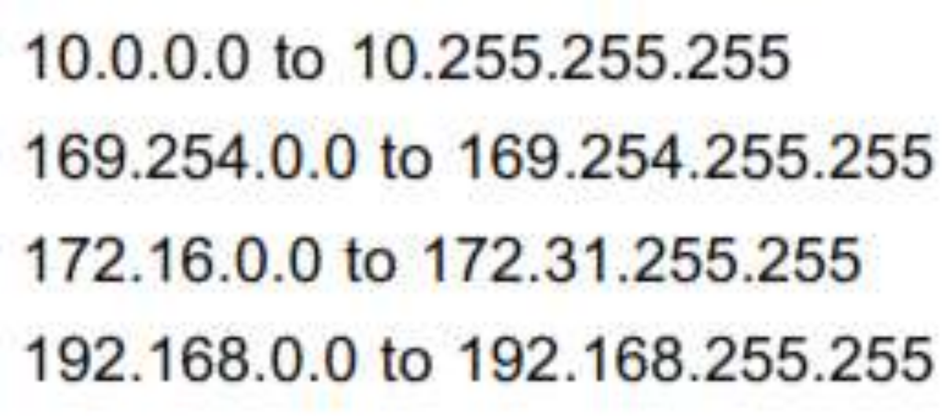
- Send : wraps the TCP datagram in its own IP datagram containing a sender’s and a receiver’s address as well as some other information
- Receive : removes the IP datagram information and passes it to TCP which will perform the checking of the contents and reordering of information before it can be passed through the appropriate port to an application

IP addresses

- Computers use numeric addresses → IP addresses for communication
- Every computer directly connected to the internet has a unique IP address.
- IPv4 (Internet Protocol version 4)
  - ranging from 0 to 255, separated by full stops (periods) in the form 192.168.0.1
- IPv6 (Internet Protocol version 6)
  - can support a theoretical 3.4×10^{38} devices
  - extremely complex process and it has taken a long time

Reserved IP numbers

- Large blocks reserved for specific users in the early days of the internet
- Some are specifically used for ‘private’ networks



10.0.0.0 to 10.255.255.255

169.254.0.0 to 169.254.255.255

172.16.0.0 to 172.31.255.255

192.168.0.0 to 192.168.255.255

From numbers to names

- Domain Name Server (DNS) : the address is translated into a unique IP address
- Located somewhere on the internet
- IP address is attached to every IP datagram destined for each server

References

- Open University, Introduction to cyber security: stay safe online, 2016

Fakultas Informatika
School of Computing
Telkom University

THANK YOU