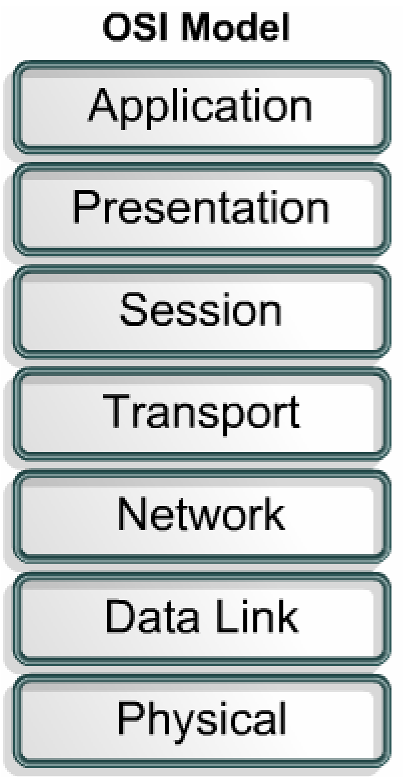
Network Security

Learning Objectives

- Network fundamentals
- Firewall technologies & securing network traffic
- Evasion techniques

Network fundamentals

The OSI model



OSI Model

Application

Presentation

Session

Transport

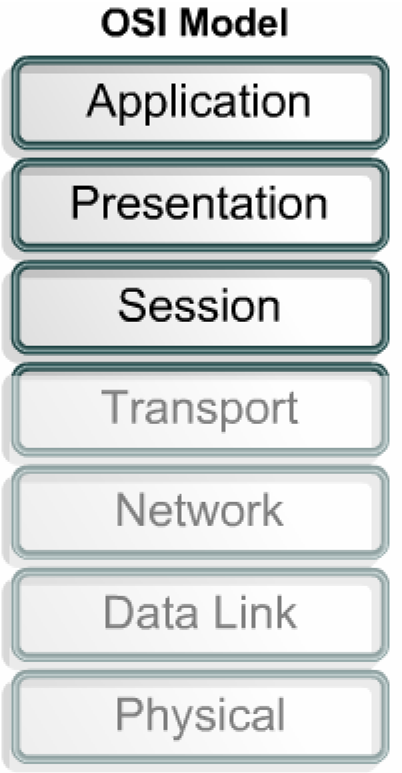
Network

Data Link

Physical

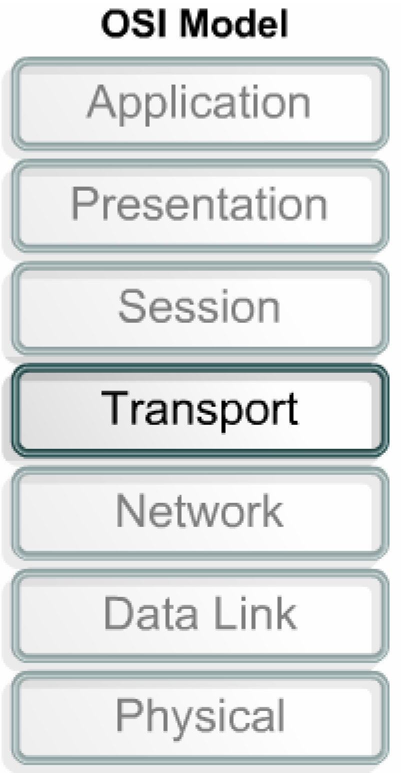
- Open Systems Interconnection (OSI) Reference Model
- Developed by ISO
  - Attempt to prompt interoperability
- A protocol defines rules
- Protocol suites define a series of protocols and interactions.
- Layers talk to each other using peer communications
- Each layer has its own protocol data unit (PDU)
  - Protocol specific information and user data

Upper layers



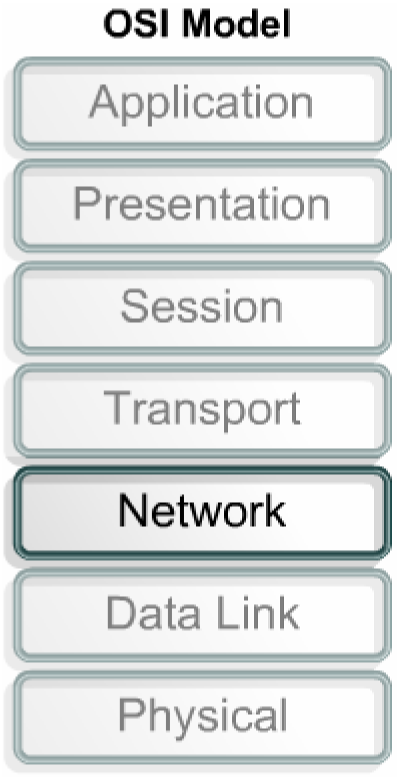
- Application: handle file transfer, virtual terminals and fulfilling networking request of applications
  - Defines what data should be transmitted
  - FTP, HTTP, Telnet, etc.
- Presentation: handle translation into standard format, data compression/decompression, data encryption/decryption
  - Specifies the way that data should be represented (ASCII, UNICODE, GIF, JPEG)
- Session: setup connection between applications; maintain control, negotiate, establish and close communication channel
  - Manages multiple transport layer connections to provide a session (consider FTP), remote procedure call (RPC)

Transport layer



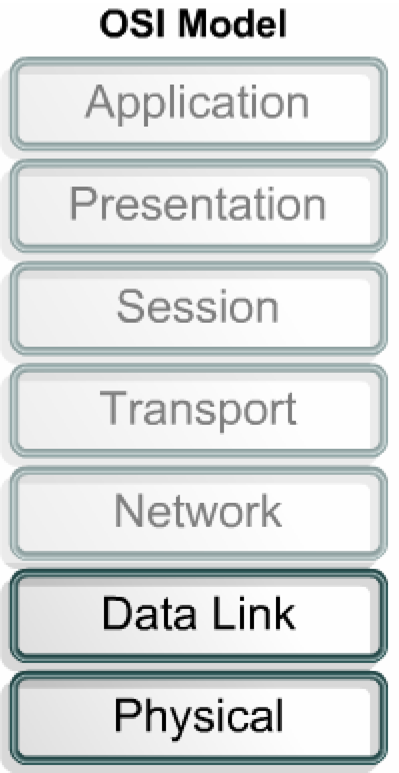
- Transport: handles end-to-end transmission and segmentation of a data stream
  - Transport services (connection and connectionless)
  - Application access points (ports)
- Main protocols
  - Transmission Control Protocol (TCP)
  - User Datagram Protocol (UDP)
  - Secure Sockets Layer (SSL)
  - Sequence Packet Exchange (SPX)

Network layer



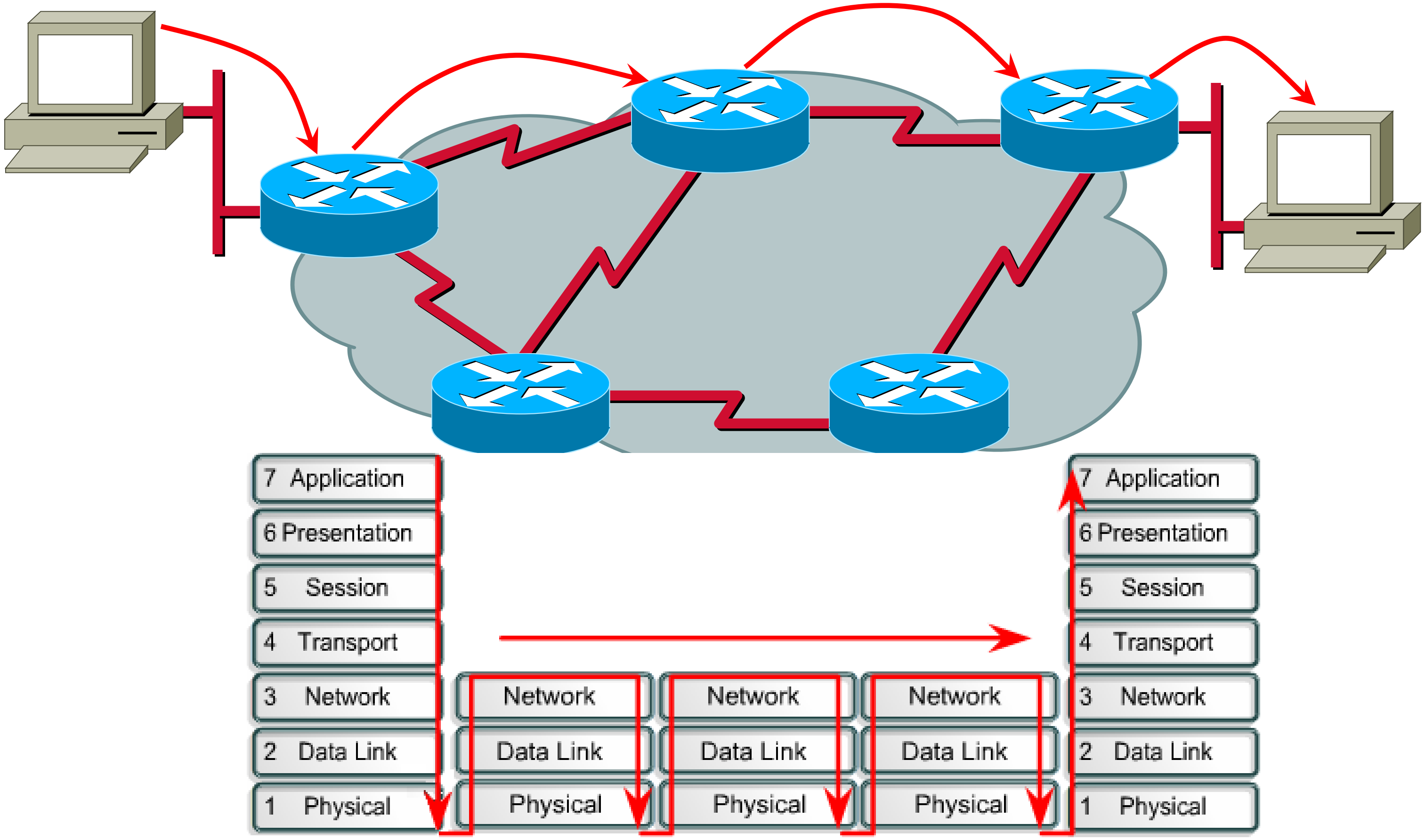
- Insert information into the packet’s header to be properly addressed and routed
- Network layer defines
  - Logical network addressing
  - Packet formats
  - Logical network structure
- Common protocols
  - Internet Protocol (IP)
  - Internet Control Message Protocol (ICMP)
  - Routing Information Protocol (RIP)
  - Open Shortest Path First (OSPF)
  - Internet Group Management Protocol (IGMP)

Lower layers



- Data Link: convert data into LAN or WAN frames for transmission and define how a computer accesses a network
  - Logical topology
  - Framing format
  - Protocols: Address Resolution Protocol (ARP), reverse ARP, point to point protocol (PPP).
- Physical layer converts bits into voltage for transmission
  - Physical topology
  - Electrical signals
  - Signalling methodologies
  - Data rates

Routers and routing



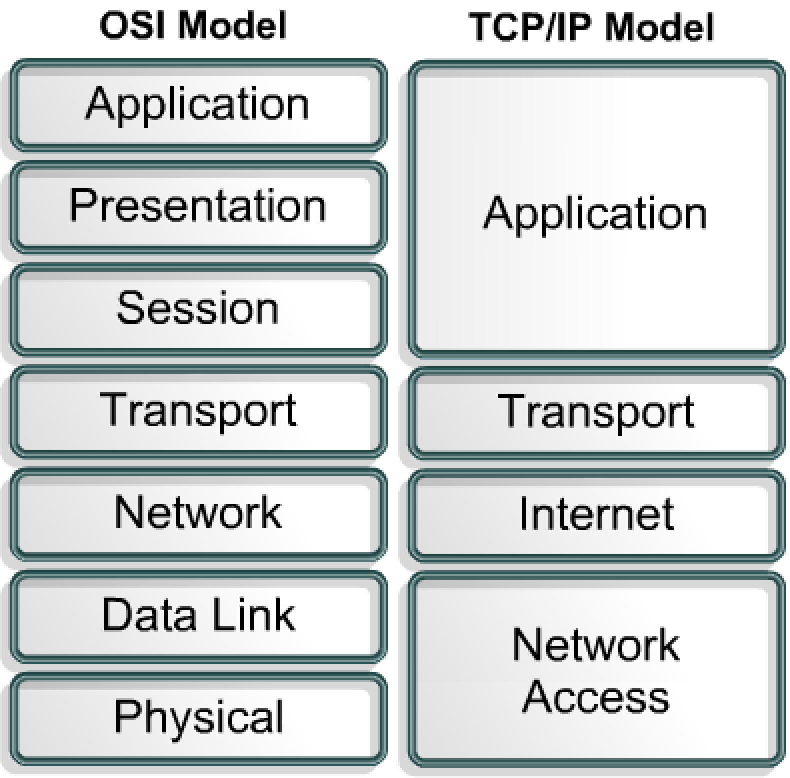
7 Application				7 Application
6 Presentation				6 Presentation
5 Session				5 Session
4 Transport				4 Transport
3 Network	Network	Network	Network	3 Network
2 Data Link	Data Link	Data Link	Data Link	2 Data Link
1 Physical	Physical	Physical	Physical	1 Physical

TCP/IP Model

- TCP/IP proposed in 1978
- Network and transport for ARPANet
  - Official protocol in 1981
- Design Goals
  - Hardware independence
  - Built in failure recovery
  - Fault tolerant
  - Efficient
  - Expandable
- TCP/IP became popular through distribution of Berkley Software Distribution (BSD) of UNIX.
- Open specification through the IETF and RFCs

TCP/IP layers

- Internet Layer
  - IP
  - ICMP
  - Routers and Routing
- Transport Layer
  - User Datagram Protocol
  - Transmission Control Protocol
  - Provides end to end transport services



Firewalls

- Packet Filtering
- Stateful Inspection/dynamic filtering
- Proxies

Packet filtering

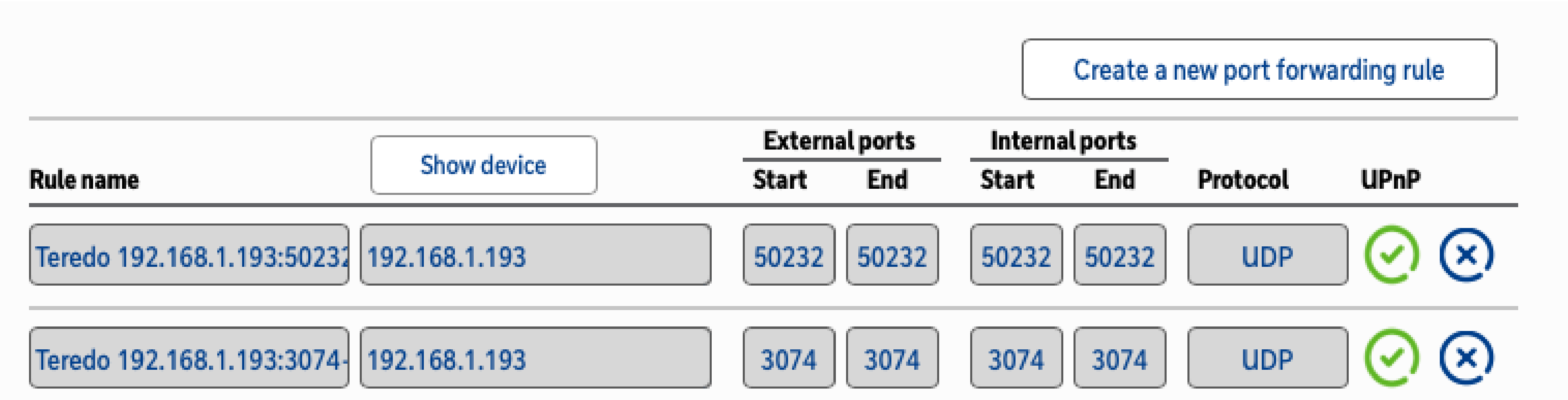
- Access Control Lists
- Based on network layer information
- Examine the header
- Weaknesses:
  - Cannot prevent attacks using the layers above, e.g. application,
  - Logging typically limited
  - Prone to improper configuration
- Example, permit udp host 10.1.1.3 host 172.16.1.2

Stateful Inspection

- Works at the transport and network layers
- Maintains a state table of communications channels
- Checks if connection had been established first. If not, it uses its ACL
- Example: iptables -A INPUT -i eth0 -m state –state \ ESTABLISHED,RELATED -j ACCEPT

uPNP

- Ports 0-1023 allocated to server side services
- Need for client to use higher ports
- How do we cope with the dynamic selection of ports?



Create a new port forwarding rule

Rule name	Show device	External ports		Internal ports		Protocol	UPnP	
		Start	End	Start	End			
Teredo 192.168.1.193:50232	192.168.1.193	50232	50232	50232	50232	UDP	✓	☒
Teredo 192.168.1.193:3074-	192.168.1.193	3074	3074	3074	3074	UDP	✓	☒

Proxy firewalls

- Second generation firewalls
- Resides between a trusted and an untrusted network
- Application level:
  - Inspects the packet up to the application layer
  - Must understand the protocols
- Circuit level:
  - Creates a circuit at the session layer between the client and proxy server
  - Makes decisions based on source and destination.
- Degrades traffic performance

Network layer

Some of the differences

- IPv6 increases IP address size from 32 bits to 128 bits
- Some IPv4 headers have been dropped or made optional to reduce processing cost of packet handling and limit bandwidth
- New type of address called ‘anycast address’ is defined, which is used to send a packet to any one of a group of nodes
- New capability to enable the labelling of packets belonging to particular traffic flows – QoS or ‘real-time’ service
- Extensions to support authentication, data integrity, and (optional) data confidentiality

IPv6 and Security

- The good (almost):
  - IPSec was mandatory for all IPv6 stack implementations
    - Has been downgraded to a recommendation
- The bad:
  - Immature protocols = increased vulnerability
  - Unfamiliarity causes problems / misconfigurations
  - Automatic addressing may pose privacy concerns
  - IPv6 security controls lagging behind hacking arsenal / tools

IPSec

- Industry standard
- Main components
  - Security protocol
    - Authentication Header (AH)
    - Encapsulation Security Payload (ESP)
  - Security Association (SA)
  - Key management: Internet Key Exchange (IKE)
  - Algorithm

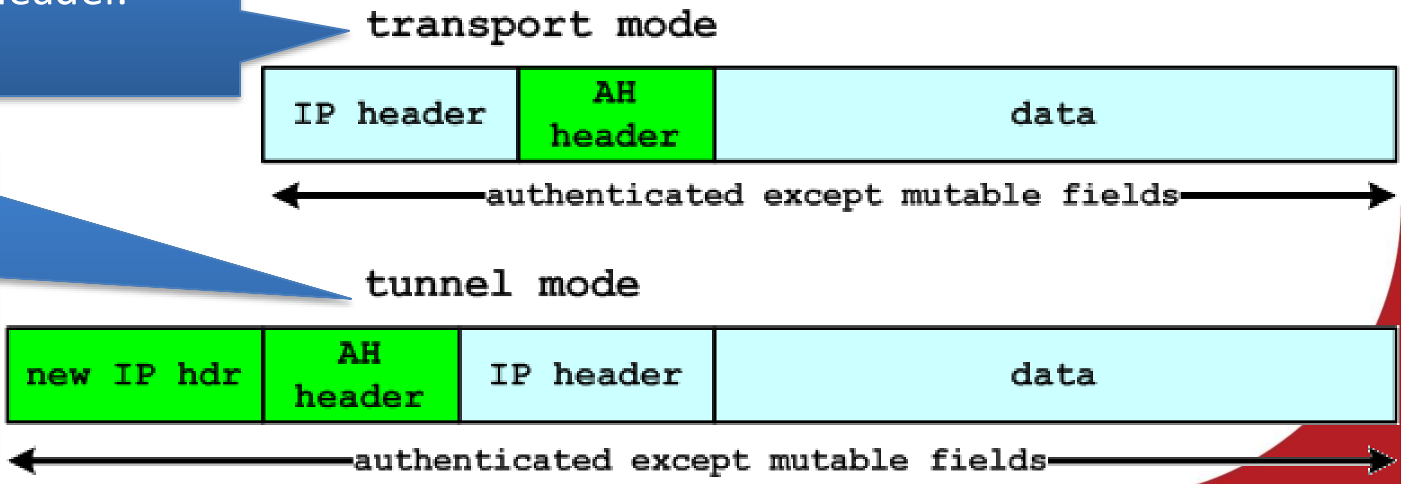
AH protocol

- AH can provide
  - Data integrity
  - Origin authentication
  - Anti-replay protection (optional)

- AH cannot provide
  - Data confidentiality
- Use for data integrity in cases where data is not secret but must be authenticated

Protects the payload and not mutable fields in the IP header.

Provides integrity and data origin authentication for the entire IP packet including the header.



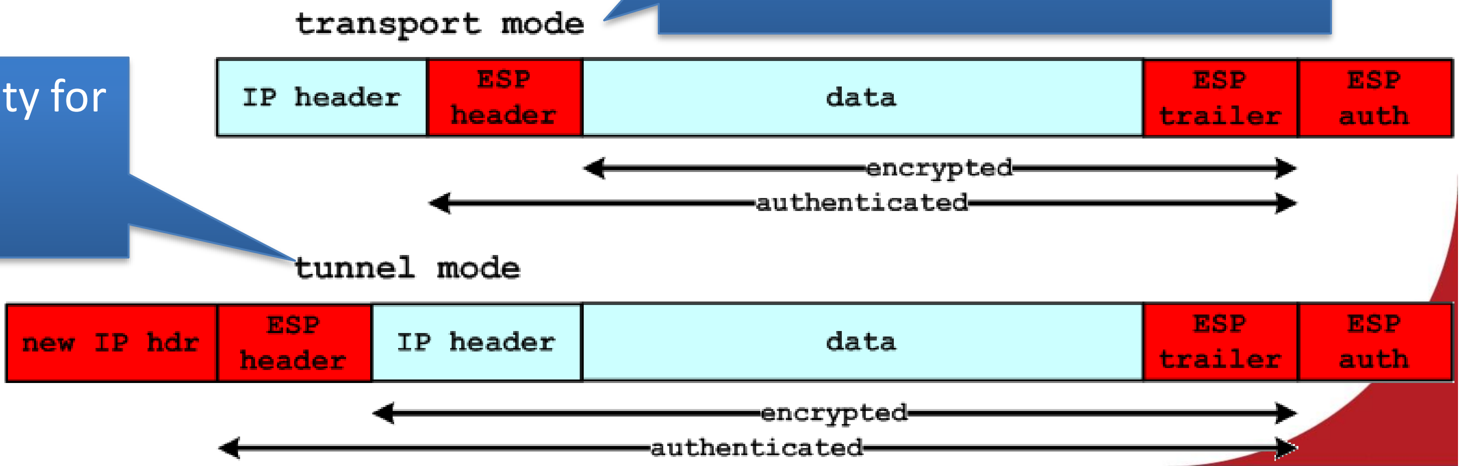
ESP protocol

- ESP can provide
  - Data confidentiality through encryption
  - Data integrity
  - Origin authentication
  - Anti-replay

- ESP doesn’t protect the IP header
- Use when data must be kept secret.

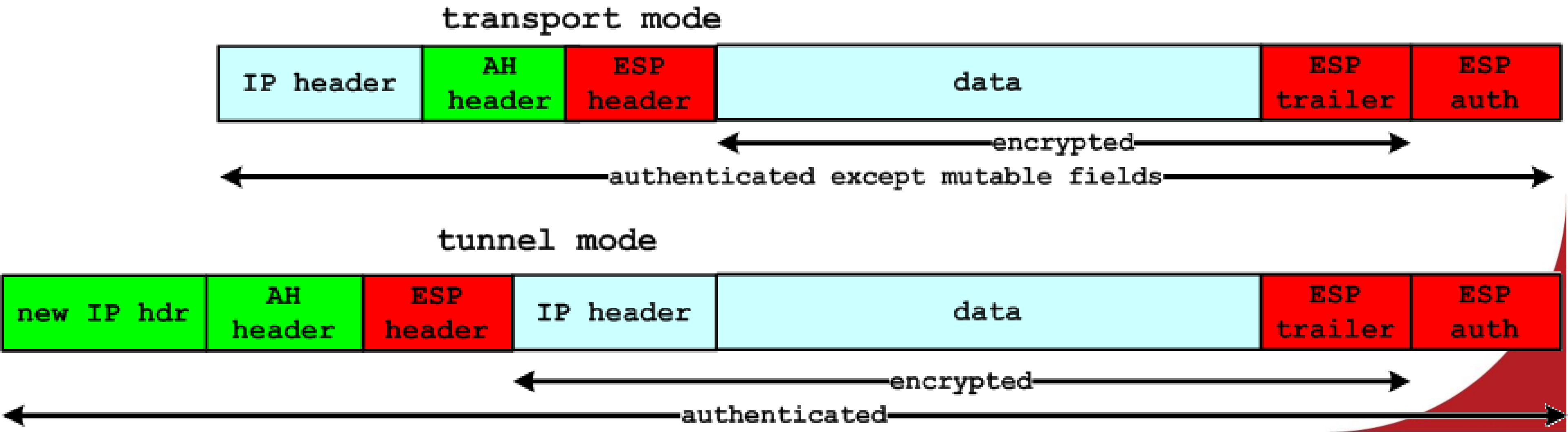
Provides confidentiality for only the payload of an IP packet.

Provides confidentiality for the entire IP packet including the header.



AH and ESP

- Using both AH & ESP can provide protection for the IP header and encrypt data.
  – Rarely used because of overhead incurred by AH.
- Use for the highest security.



Evasion techniques

Methods to avoid detection

- Anonymity
- Unobservability

https://www.freehaven.net/anonbib/cache/terminology.pdf

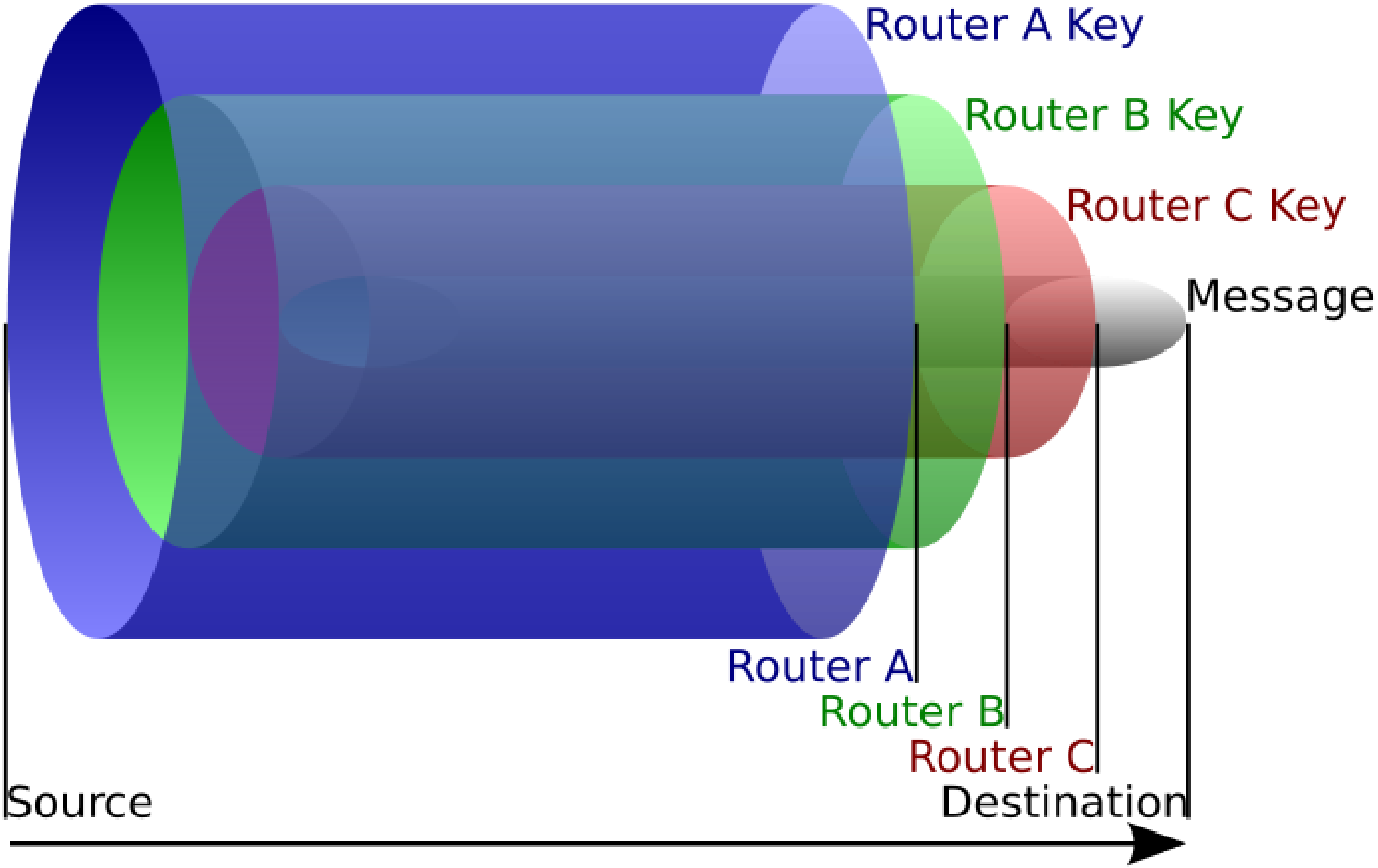
End-to-end anonymity

- Use of distributed, anonymous networks
  - The Tor Project (https://www.torproject.org/)
  - The Invisible Internet (I2P) (https://geti2p.net/)
  - Freenet (https://freenetproject.org/)

The Tor network

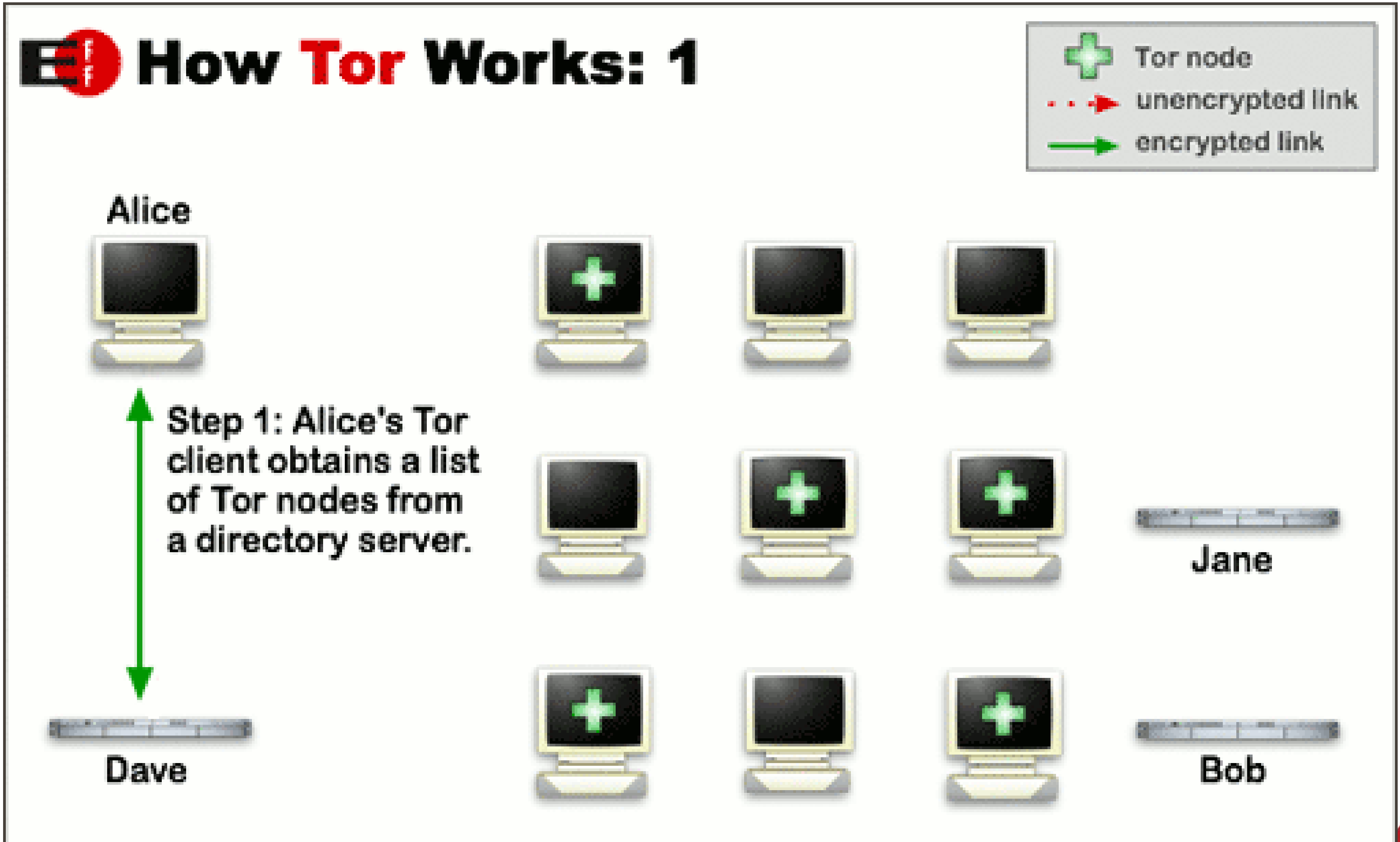
- What is it?
  - A distributed anonymous communication service.
  - It is using an overlay network to improve anonymity on the Internet.
- Its design
  - Onion Routers (OR) route traffic
  - Onion Proxy (OP) fetches directories and creates virtual circuits.
  - Use of TCP with TLS.
  - Data is sent in fixed size (bytes) cells.

The onion routing protocol



https://en.wikipedia.org/wiki/Onion_routing

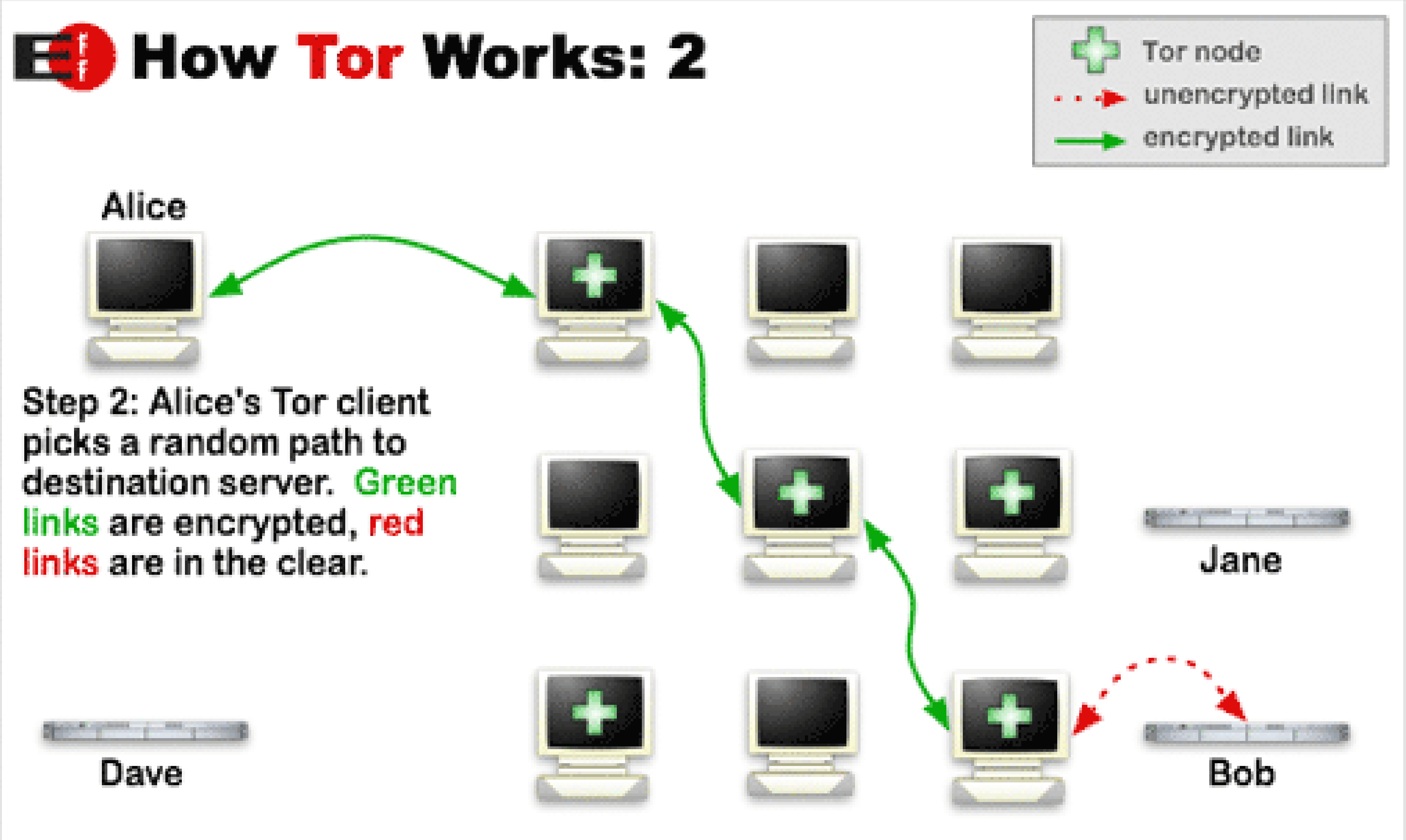
How Tor works



Step 1: Alice's Tor client obtains a list of Tor nodes from a directory server.

https://2019.www.torproject.org/about/overview.html.en

How Tor works

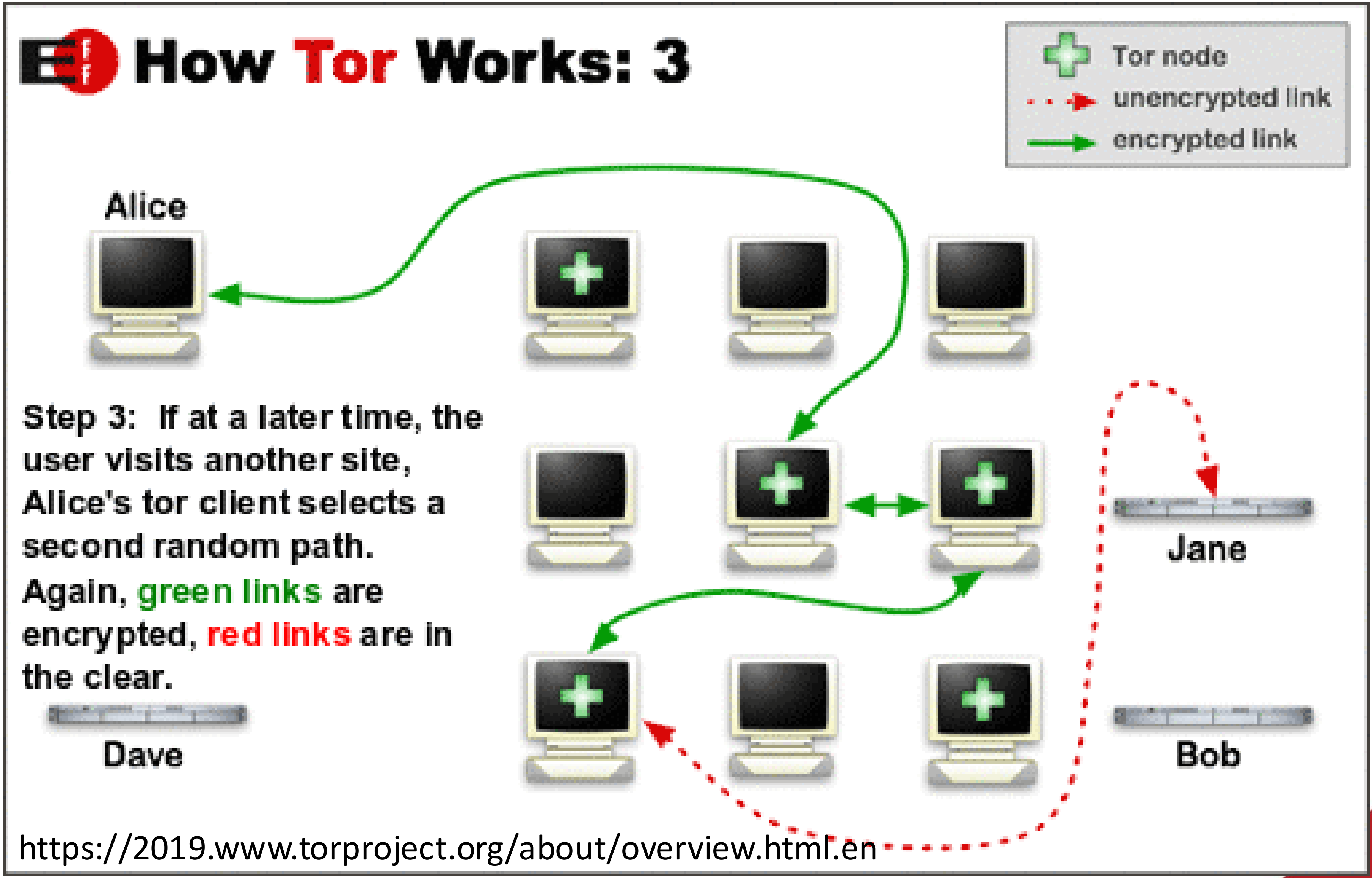


How Tor Works: 2

Step 2: Alice's Tor client picks a random path to destination server. Green links are encrypted, red links are in the clear.

https://2019.www.torproject.org/about/overview.html.en

How Tor works



Step 3: If at a later time, the user visits another site, Alice's tor client selects a second random path. Again, green links are encrypted, red links are in the clear.

https://2019.www.torproject.org/about/overview.html.en

Threats in Tor

- DNS leaks
  - DNS requests are not sent via the Tor network by default. Thus, an attacker could see what websites are being visited.
- Traffic analysis
  - Tor is vulnerable to an attacker who can see both ends of a connection.
- Malicious exit nodes
  - Traffic from the exit node to the target is not encrypted.

Questions?

References

- CISSP All in One. Chapter 7 Telecommunications and Network Security.
- Internet Protocol RFC 791
- Transmission Control Protocol RFC 793