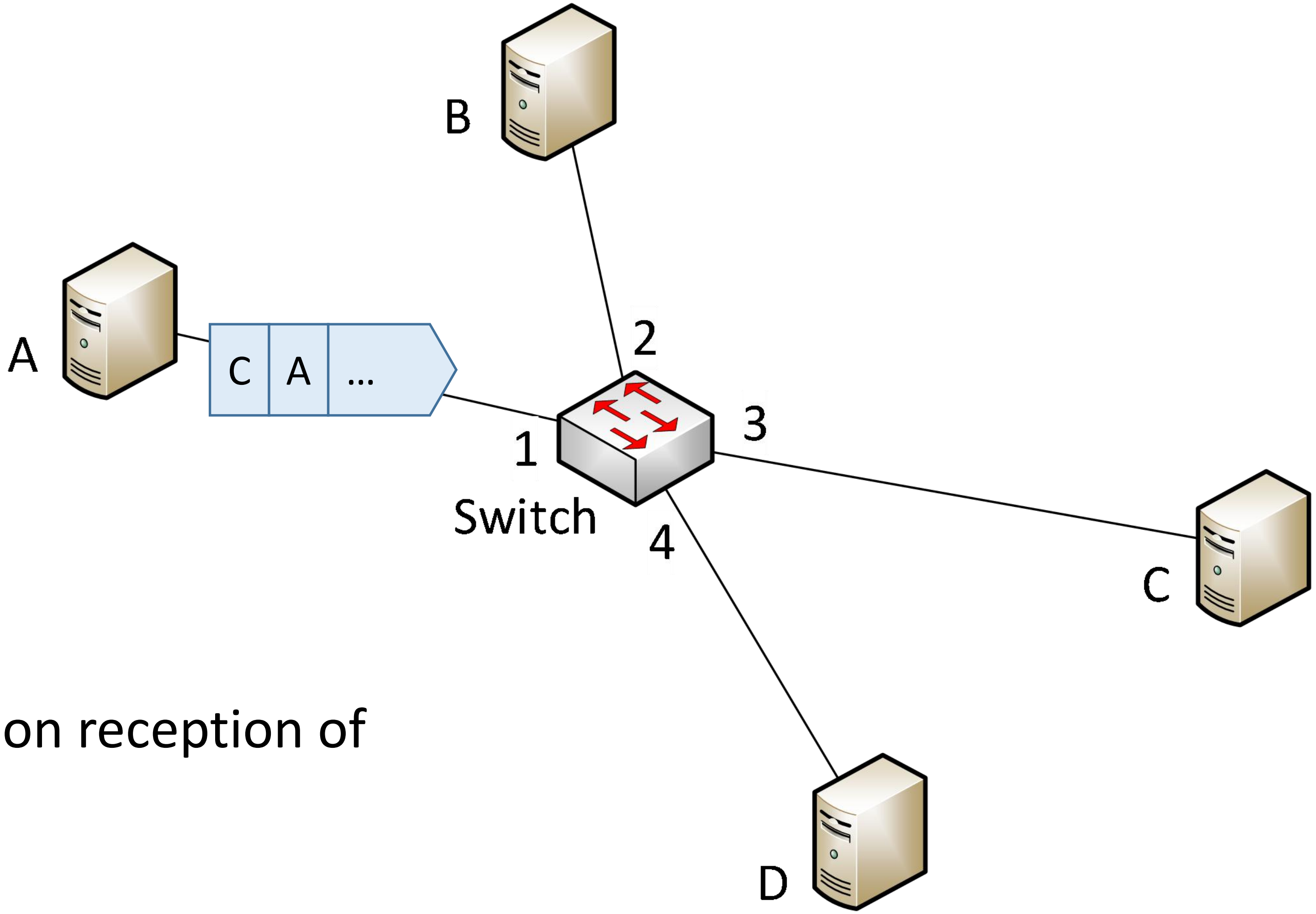
Computer Networks

Computer Network Security

Threats to Switching

Port stealing

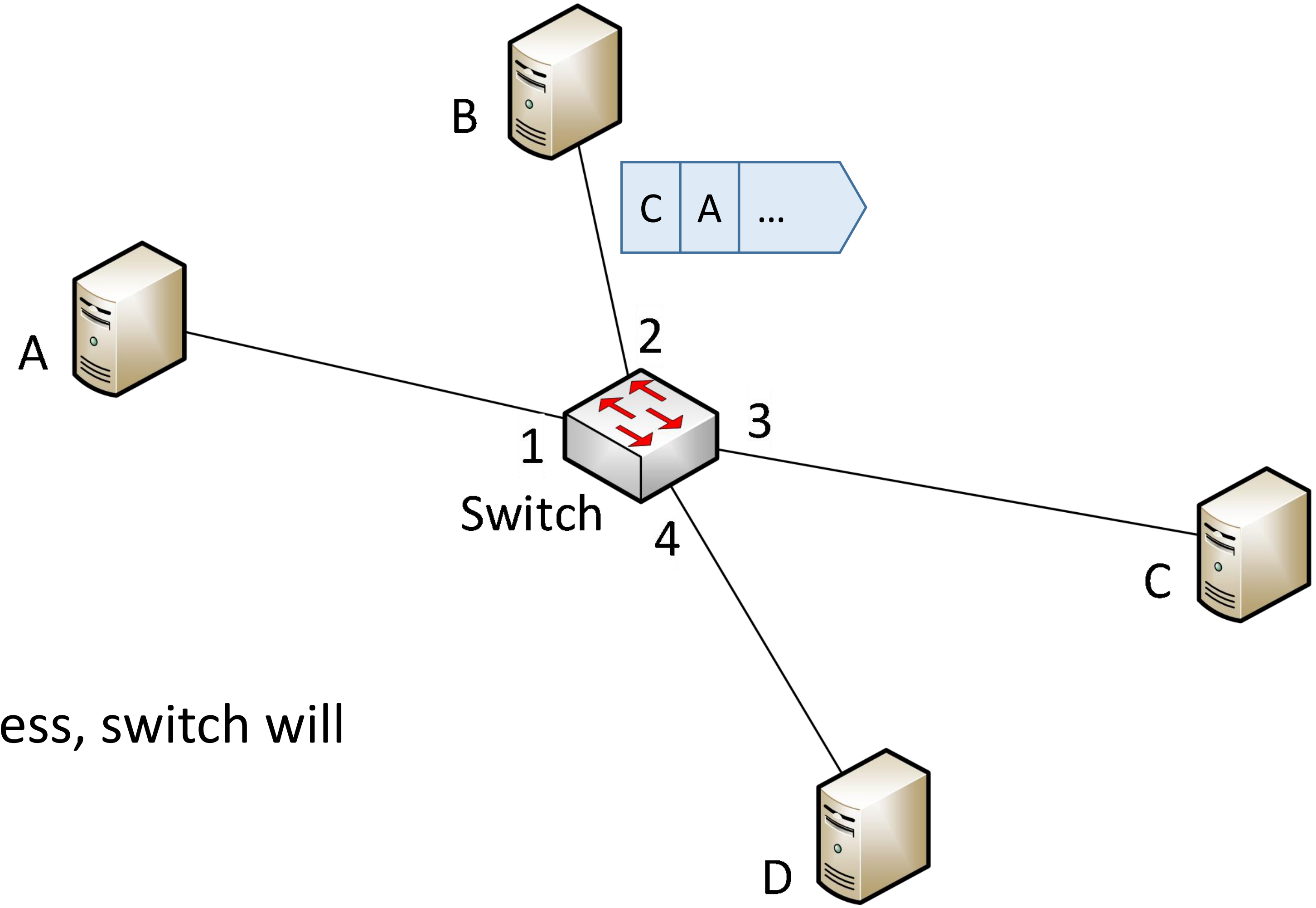
Forwarding Information Base	
MAC address	Interface No
A	1
C	3



Switch learns MAC addresses upon reception of any frame

Port stealing

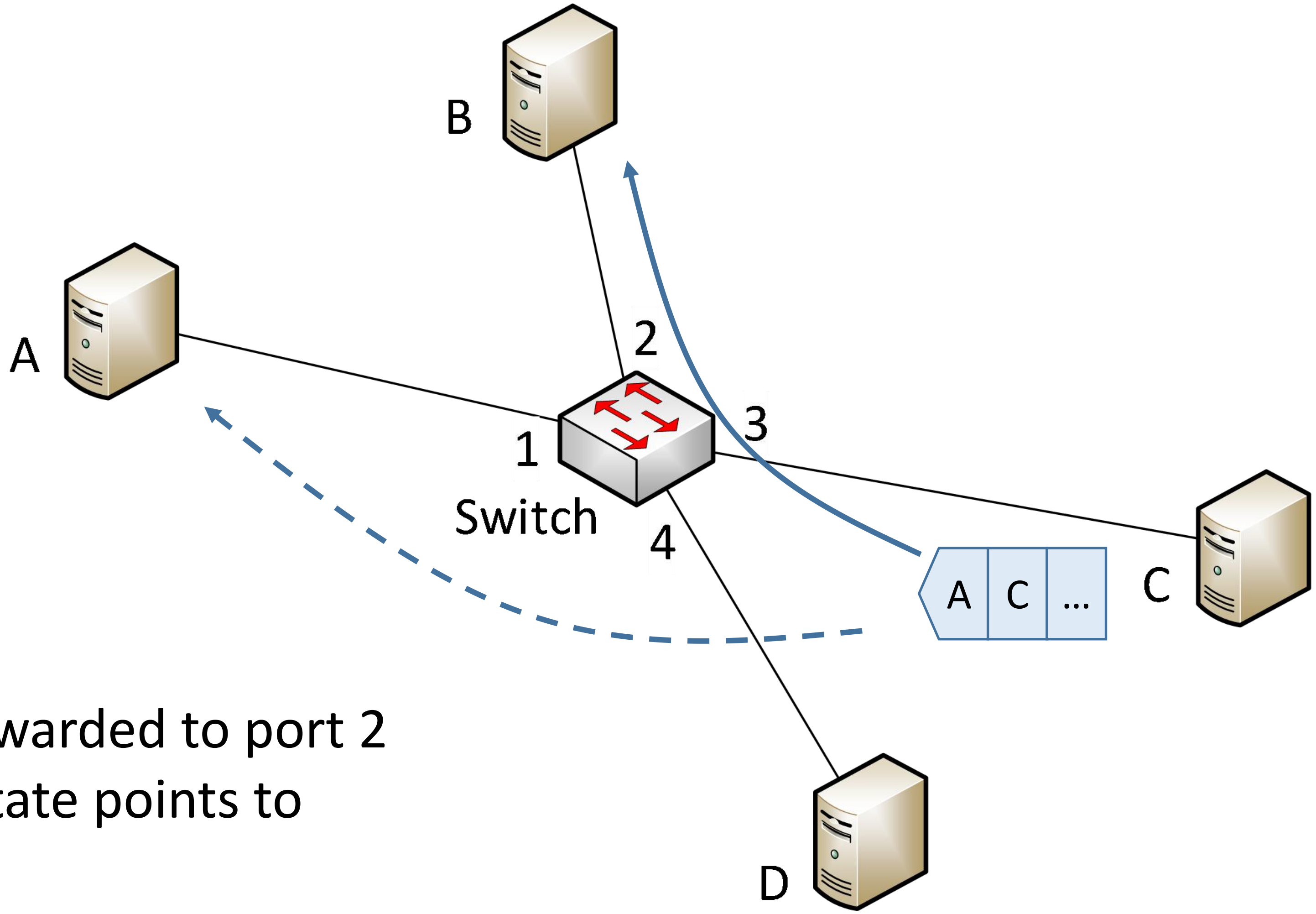
Forwarding Information Base	
MAC address	Interface No
A (spoofed by B)	2
C	3



If station B spoofs A’s MAC address, switch will learn that A is present on port 2

Port stealing

Forwarding Information Base	
MAC address	Interface No
A (spoofed by B)	2
C	3



Station C’s responses will be forwarded to port 2 instead of port 1 if current FIB state points to port 2

FIB (CAM) Flooding

- Attack aiming in flooding the Forwarding Information Base – table looked up in switching process
- According to switching rules, if an entry is not found in the table, frame is switched as to an unknown destination
- The aim is to fill the table with useless MAC entries so that every genuine MAC address is treated as unknown -> broadcasted to all ports
- Quite „noisy” attack – large volume of unsolicited traffic may be observed and easily tracked down
- Leads to information leak

FIB (CAM) Flooding – mitigation

- Attack can be mitigated somehow by using encrypted traffic
- Inside LAN segment this is not popular for many protocols, excluding HTTPS

Selected other low-level LAN threats

- Spanning-Tree Protocol manipulation
  - many mitigation measures exist
- VLAN tagging manipulation
  - ultimate solution exist

STP manipulation – mitigation

VLAN tagging manipulation

VLAN tagging manipulation – mitigation

ARP spoofing

- In general aims in creating a fake entry in victim’s ARP table
- The entry typically leads to an attacker station instead of a genuine one
- Typically performed against default gateways
- As a result traffic from victim’s computer is switched to attacker station instead
- Attacker then inspects/manipulates the traffic and sends further to proper station
- If performed against the whole LAN segment, broadcast addresses may be used

Smart spoofing

- An example of Man-in-the-Middle attack (MitM)
- Performed using only unicast frames
- No broadcast manipulation is observed
- Manipulates every single victim in a LAN segment
- In the smallest case, only two nodes are manipulated – the victim and the default gateway
    - this gives the attacker access to bi-directional communication channel, hence the MitM case
- Mechanics of the attack remain the same as for typical ARP spoofing

ARP/Smart spoofing mitigation

- In general it is infeasible in many scenarios to totally mitigate the threat
- In some cases static ARP entries may help
  - no queries are performed for specific IP addresses
  - hard to manage settings on all the other network nodes
  - make network card replacement a hard task
  - the use of virtual MAC addresses may help to some extent

Overlay security in computer networks

Overlay security concept

- Network solution available in lower layers may lack security measures
  - various security properties may be missing: e.g. confidentiality, availability
- An overlay security measure should be able to tolerate these imperfections
  - if a protocol can be sniffed, an encryption should be provided
  - if spoofing is possible, (mutual) authentication sholud be provided
  - if datagram removal is possible, redundancy should be provided

Network protocols insecurities at a glance

- The following cases are just the examples crucial protocol functionality impact; in general sniffing, spoofing and denial of service (DoS) possible in all cases
- IPv4/IPv6
  - sniffing, spoofing
- ARP
  - spoofing
- DNS
  - sniffing, spoofing
- DHCP
  - DoS
- routing
  - spoofing, DoS
- HTTP
  - spoofing

AAA protocols

- AAA:
  - Authentication – checking who are we talking to
  - Authorization – knowing to whom we talk, give them the right privileges
  - Accounting – to count how many various resources they’ve consumed
- RADIUS
  - the most popular AAA protocol
  - some point out its limited authentication capabilities
  - available in the majority of enterprise-grade network solutions
- Diameter
  - an upgraded version of RADIUS
  - much higher functionality, improved security

AAA protocols

- LDAP
  - directory services oriented – divides network resources into group types, allows for logical resource grouping
  - not quite an AAA protocol, provides authorization in general
  - sometimes used in exchange of RADIUS
- All the mentioned AAA protocols are not self-reliant
  - make use of many other protocols like EAP variants, Kerberos, etc.

TLS – Transport Layer Security

- An improved version of SSL protocol (Secure Socket Layer)
- Used in OSI layer 4 as an secure extension of typical protocols
  - SMTP – SMTPS
  - IMAP – IMAPS
  - FTP – FTPS
  - HTTP – HTTPS
- ALPN – Application-Layer Protocol Negotiation
  - extension allowing for the generalization to other protocols
- Allows for authentication of at least one communication party
- Sometimes used directly in proposed protocols, e.g. VPN ones

TLS in connectionless communication

- connectionless communication makes it harder to attribute datagrams to a distinct session
- example applications
  - DNS
  - NTP
  - SNMP
  - RADIUS
  - stream traffic
  - tunneling – VPN
  - HTTP over QUIC, HTTP/3
- DTLS – Datagram TLS
  - solution devoted to datagram traffic, UDP in particular

VPN solutions

- VPN – Virtual Private Network
- Are example of an overlay security measure
- Originally used to interconnect two LAN segments over untrusted WAN network
- May be used in one of two variants:
  - site-to-site – the original applications, make use of so-called VPN gateways (devices responsible for VPN tunnel management)
  - client-to-site: between a user and VPN gateway
- Provide authenticity, confidentiality, integrity but not availability in general

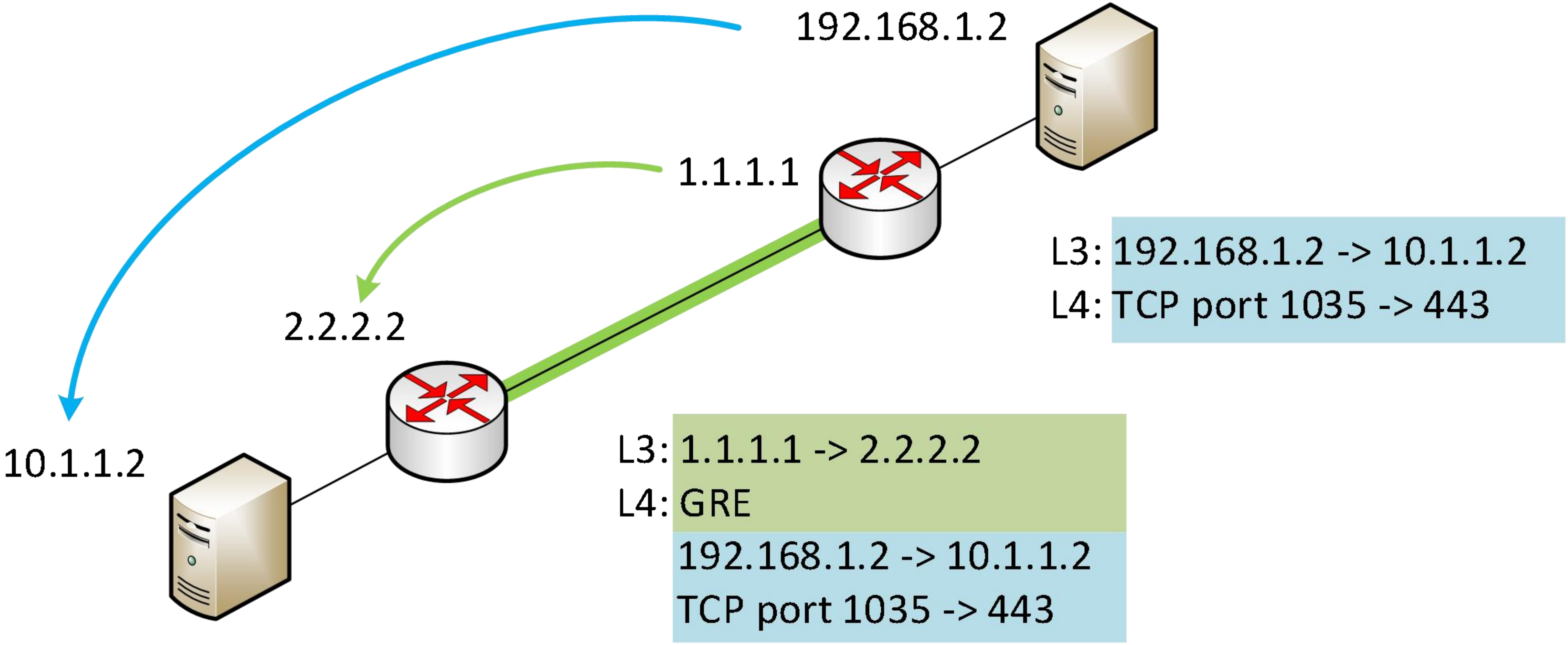
VPN mode of action

1. mutual authentication
2. crypto-material agreement – common secret as a result on both sides
3. data encryption – encapsulation
4. management of crypto material – periodical exchange of stream keys etc.

Standarized VPN solutions

- IPsec – IP security
  - many RFC documents
  - relatively complex
  - allows for precise control over security measures in every step of VPN establishment
- L2TP
  - RFC 2661, RFC 3931
  - uses UDP
  - not self-reliant at present
- GRE – Generic Routing Encapsulation
  - RFC 1701, RFC 1702, RFC 2784
  - not self-reliant, does not provide authentication nor encryption
- PPTP – just informative RFC 2637, originally proprietary, compromised

VPN – encapsulation



L3: 192.168.1.2 -> 10.1.1.2
L4: TCP port 1035 -> 443

L3: 1.1.1.1 -> 2.2.2.2
L4: GRE
192.168.1.2 -> 10.1.1.2
TCP port 1035 -> 443