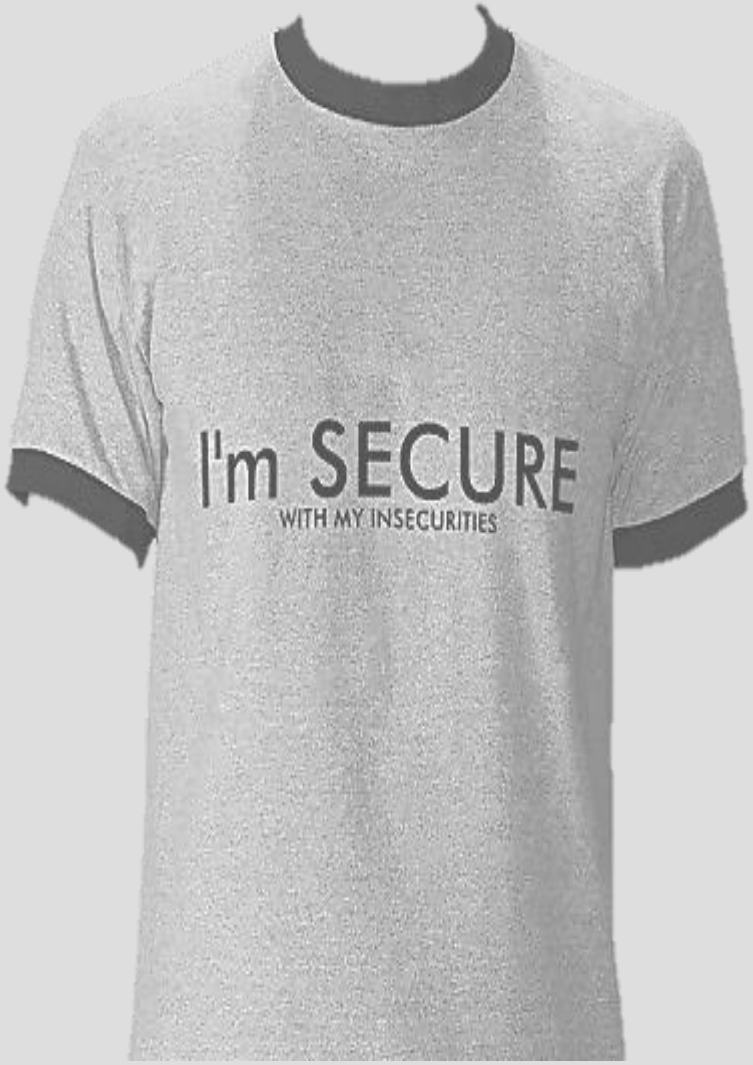
Secure Communications & Cryptography

Networking 101



Mark Cummins
Institute of Technology Blanchardstown
mark.cummins@itb.ie
+353 1 885 1156

Securing Network Traffic

- To understand how safe or vulnerable our information is when we send it across the network we need to understand exactly how it is sent.

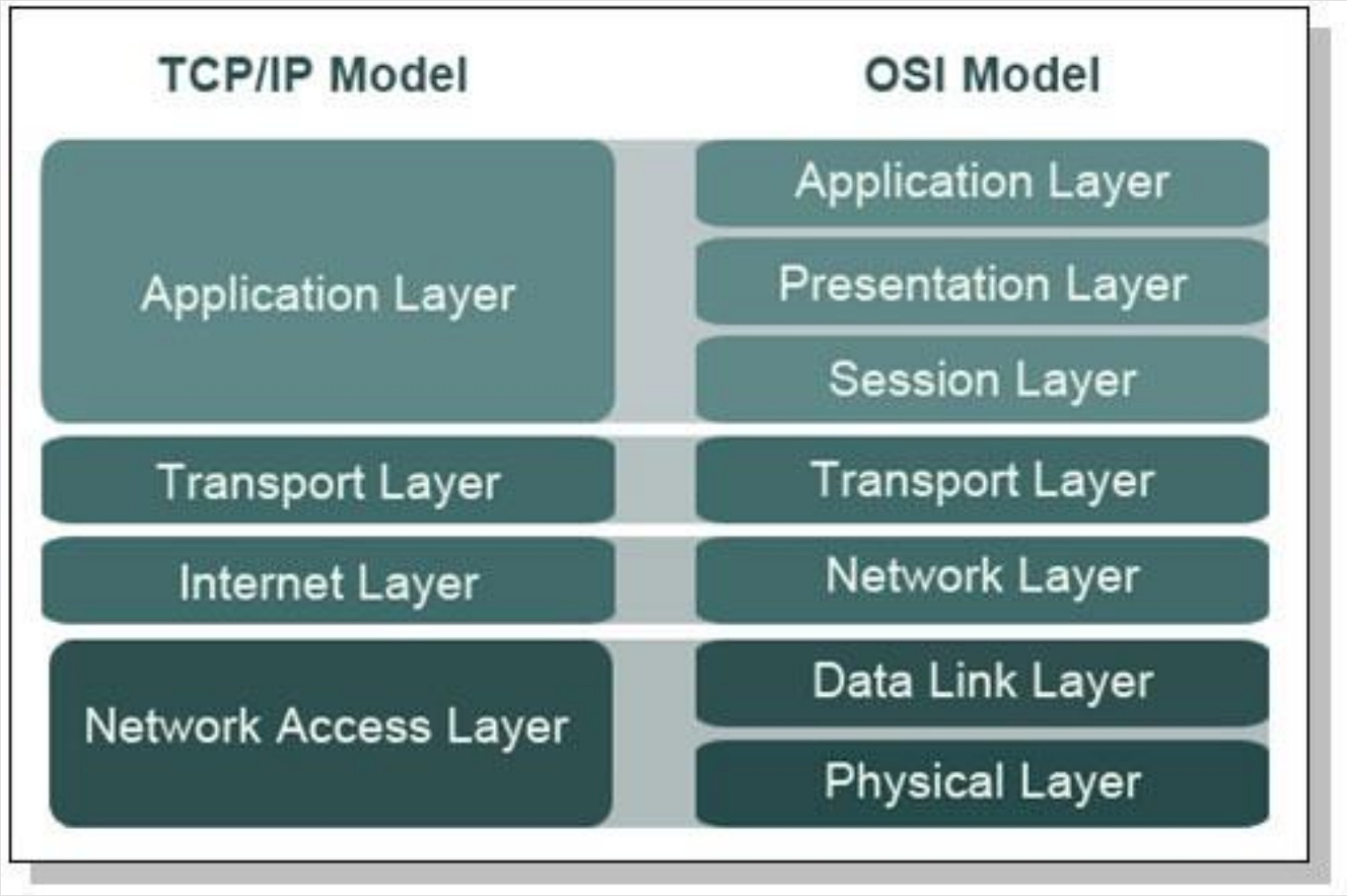
Mark Cummins
Institute of Technology Blanchardstown
mark.cummins@itb.ie
+353 1 885 1156

OSI Model

	data unit	layers
Host Layers	data	**application** Network Process to Application
	data	**presentation** Data Representation & Encryption
	data	**session** Interhost Communication
	segments	**transport** End-to-End Connections and Reliability
Media Layers	packets	**network** Path Determination & Logical Addressing (IP)
	frames	**data link** Physical Addressing (MAC & LLC)
	bits	**physical** Media, Signal and Binary Transmission

Mark Cummins
Institute of Technology Blanchardstown
mark.cummins@itb.ie
+353 1 885 1156

OSI Versus TCP/IP Model



Mark Cummins
Institute of Technology Blanchardstown
mark.cummins@itb.ie
+353 1 885 1156

Ethernet & Switched Networks

How does Ethernet Work?

Why are modern networks fully switched?

Mark Cummins
Institute of Technology Blanchardstown
mark.cummins@itb.ie
+353 1 885 1156

Wireless Versus Wired networks

- CSMA / CD (wired)
- CSMA / CA (wireless)

- Can we sniff packets like on a wired network?

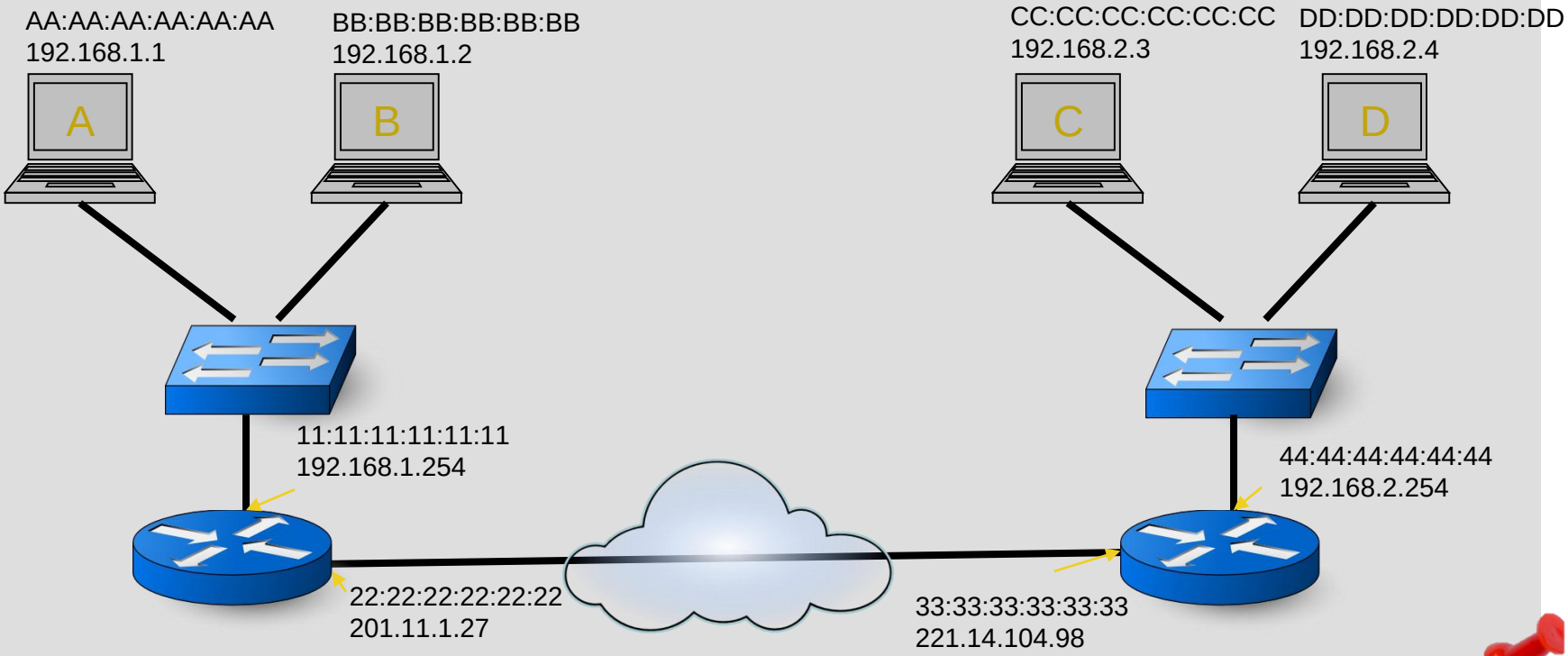
Mark Cummins
Institute of Technology Blanchardstown
mark.cummins@itb.ie
+353 1 885 1156

How is information sent across the internet?

IPsec
ARP
Telnet
ACK
HTTP
Subnet
CIDR
SYN
URL
TCP/IP
WAN
OSI
TCP
DNS
4 Layers
TLS
MAC
Transport Layer
Routers
VPN
SSL
FTP
Ethernet
LAN
SYN/ACK
7 Layers
UDP
SMTP
HTTPS
IP Addresses

Mark Cummins
Institute of Technology Blanchardstown
mark.cummins@itb.ie
+353 1 885 1156

How is information sent across the internet?



Destination MAC	Source MAC	Destination IP	Source IP

Full P2P Demo

Legacy Protocols

- All of the older protocols were concerned with getting stuff to communicate.
- Security wasn't considered, until more recently.
- These unencrypted protocols are vulnerable to numerous attacks and expose networks to attack

Mark Cummins
Institute of Technology Blanchardstown
mark.cummins@itb.ie
+353 1 885 1156

Types of attack

- Eavesdropping
  - Identity theft /
  - Packet capture
- Spoofing
  - Replay
  - Man-in-the-middle
  - Hijacking
- Denial of Service
  - DDOS
  - RDDOS

Smurf Attack

Fraggle Attack

Mark Cummins
Institute of Technology Blanchardstown
mark.cummins@itb.ie
+353 1 885 1156

Attacking Tools

- Protocol/Network analysers, Sniffers
  - Wireshark

- Network mappers port scanners
  - Nmap

Sniffing on switched networks

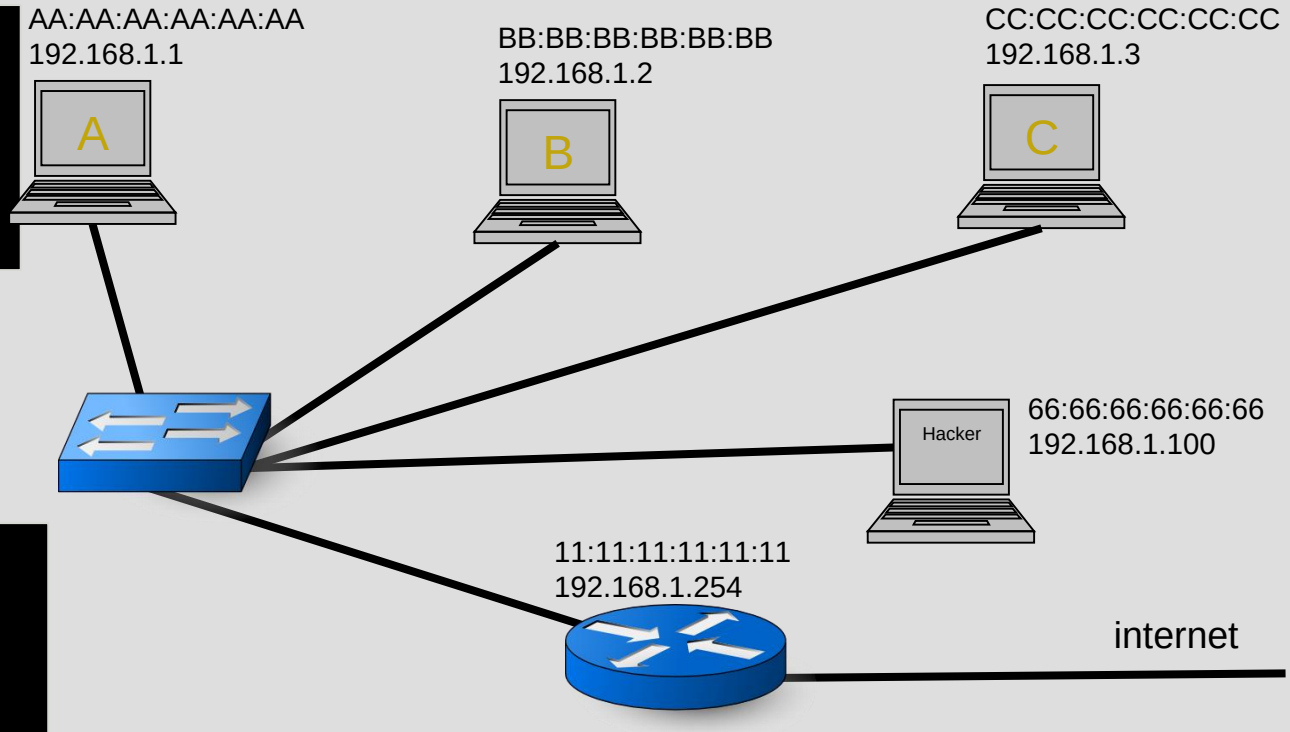
- So how can we sniff traffic on a switched network?
- How does ARP work?

MAC Flooding
+ ARP
Poisoning

Sniffing on a switched network

ARP Table – PC A

192.168.1.2 BB:BB:BB:BB:BB
192.168.1.254 11:11:11:11:11:11



CAM Table – Switch

Port 1	AA:AA:AA:AA:AA
Port 2	BB:BB:BB:BB:BB
Port 3	CC:CC:CC:CC:CC
Port 4	66:66:66:66:66:66
Port 5	11:11:11:11:11:11

Thank You