COMS 3000/7003

Week 12

Network Security

Tutor Assessments

Dear students,

UQ and ITEE takes pride in the quality of its teaching staff and encourages you to provide constructive feedback of the course tutors through the SETutor survey process. Before Saturday 22 October, 2017 please access the link below and using the password for the tutors you have had contact with this semester complete the online survey.

Tutor Assessments

Link: https://eval.uq.edu.au/	
Tutor:	**Password:**
Mr Kristan Edwards	TT2ES
Dr Kaleb Leemaqz	5ZPFQ

Thank you, your cooperation is appreciated.

(ISC)²® CISSP® Domains

- The CISSP CBK consists of 8 domains (used to be 10):
- **Security and Risk Management**
- **Asset Security**
- **Security Engineering (Physical + Crypto)**
- **Communication and Network Security**
- **Identity and Access Management**
- **Security Assessment and Testing**
- **Security Operations**
- **Software Development Security**

PCI Data Security Standard

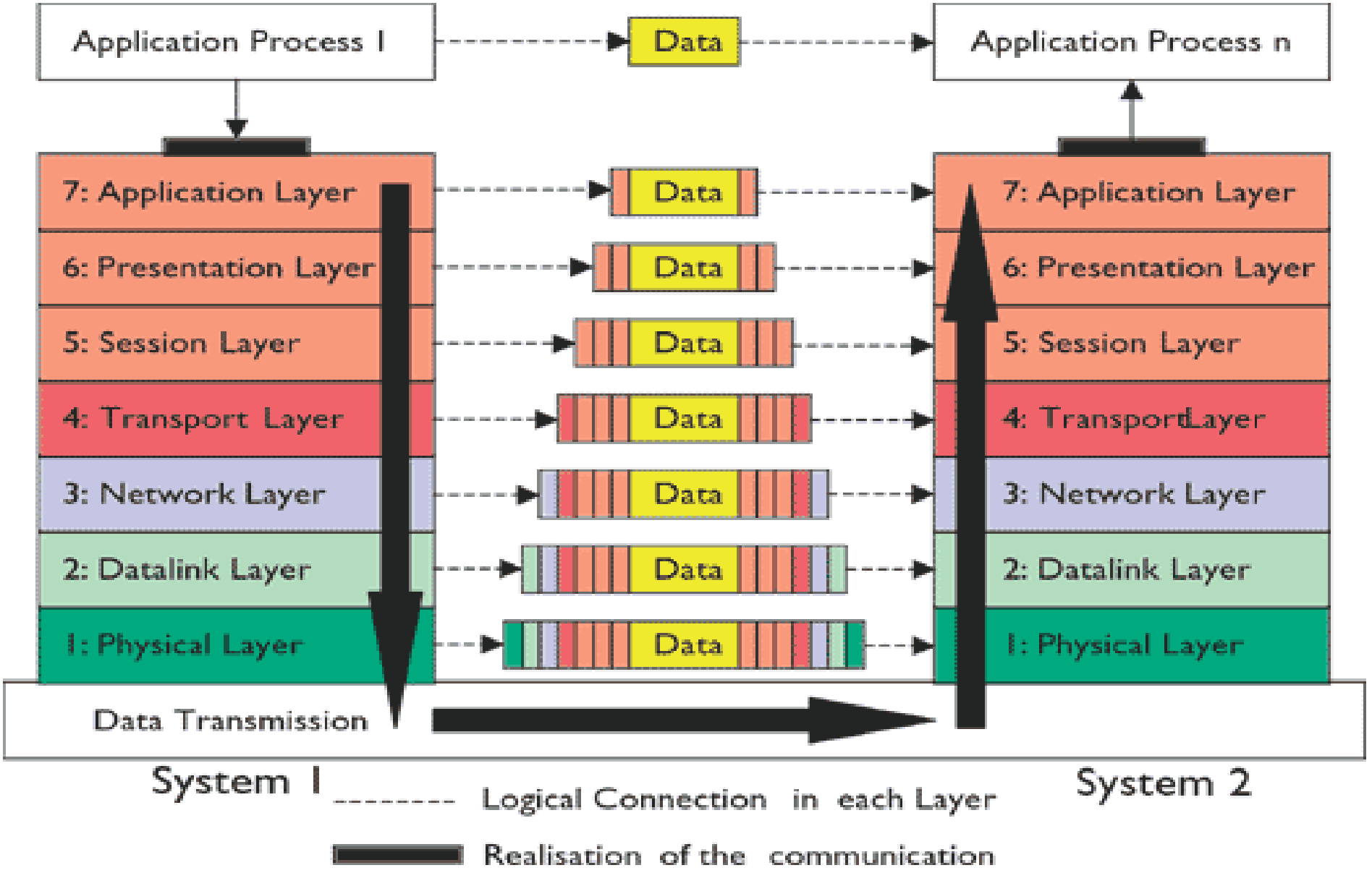
- Build and Maintain a Secure Network
  - 1. Install and maintain a firewall configuration to protect cardholder data
  - 2. Do not use vendor-supplied defaults for system passwords and other security parameters
- Protect Cardholder Data
  - 3. Protect stored cardholder data
  - 4. Encrypt transmission of cardholder data across open, public networks
- Maintain a Vulnerability Management Program
  - 5. Use and regularly update anti-virus software or programs
  - 6. Develop and maintain secure systems and applications
- Implement Strong Access Control Measures
  - 7. Restrict access to cardholder data by business need-to-know
  - 8. Assign a unique ID to each person with computer access
  - 9. Restrict physical access to cardholder data
- Regularly Monitor and Test Networks
  - 10. Track and monitor all access to network resources and cardholder data
  - 11. Regularly test security systems and processes
- Maintain an Information Security Policy
  - 12. Maintain a policy that addresses information security for employees and contractors

PCI Data Security Standard

- Build and Maintain a Secure Network
  - 1. Install and maintain a firewall configuration to protect cardholder data
  - 2. Do not use vendor-supplied defaults for system passwords and other security parameters
- Protect Cardholder Data
  - 3. Protect stored cardholder data
  - 4. Encrypt transmission of cardholder data across open, public networks
- Maintain a Vulnerability Management Program
  - 5. Use and regularly update anti-virus software or programs
  - 6. Develop and maintain secure systems and applications
- Implement Strong Access Control Measures
  - 7. Restrict access to cardholder data by business need-to-know
  - 8. Assign a unique ID to each person with computer access
  - 9. Restrict physical access to cardholder data
- Regularly Monitor and Test Networks
  - 10. Track and monitor all access to network resources and cardholder data
  - 11. Regularly test security systems and processes
- Maintain an Information Security Policy
  - 12. Maintain a policy that addresses information security for employees and contractors

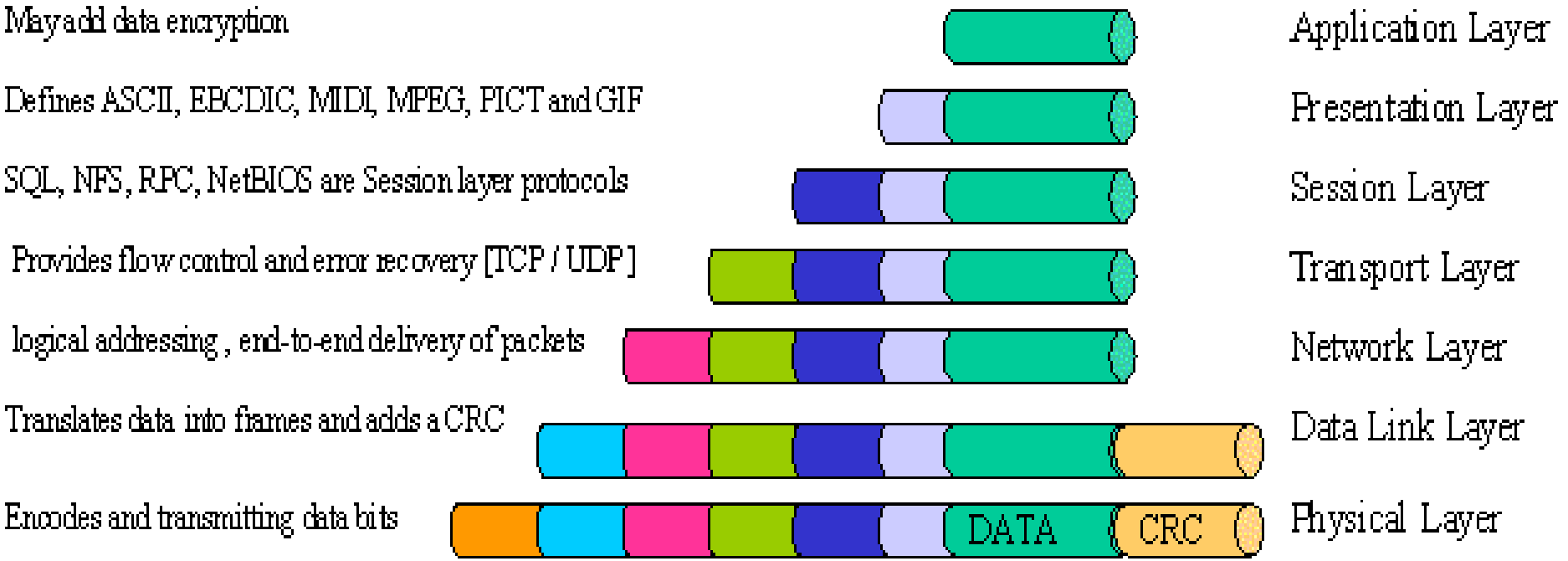
Telecommunications and Network Security

ISO's OSI Model



IEB Media GbR, "Industrial Ethernet Book" from http://www.spottek.ca/Tutorials/images/ieb23protocol1.gif

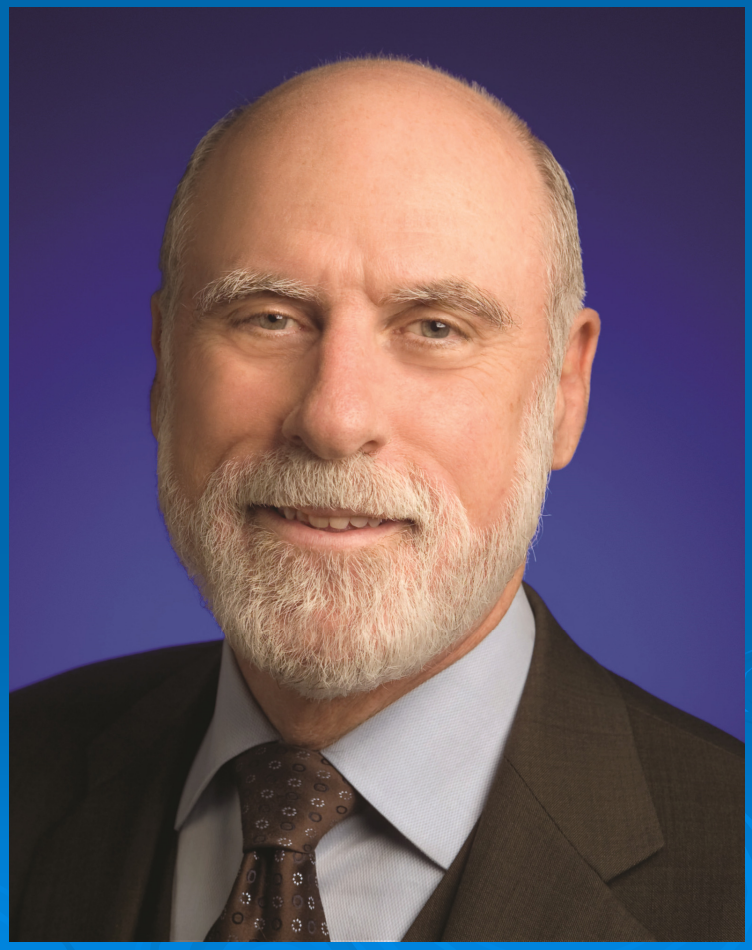
Practical OSI Layers



Leroy Davis, http://www.interfacebus.com/OSI_Stack.gif

Inventors of TCP (later TCP/IP)

Dr Robert E Kahn and Dr Vinton Cerf



commons.wikimedia.org

one of Vint's (Google?) promo shots

Layering

IEN # 2 — Jon Postel
Supercedes: None — ISI
Replaces: None — 15 August 1977

2.3.3.2 Comments on Internet Protocol and TCP

Introduction

This memo suggests an approach to protocols used in internetwork systems somewhat different from the main thrust of the work on the Transmission Control Protocol (TCP) [1]. The position taken here is that internetwork communication should be view as having two components: the hop by hop relaying of a message, and the end to end control of the conversation. This leads to a proposal for a hop by hop oriented internet protocol, an end to end oriented host level protocol, and the interface between them.

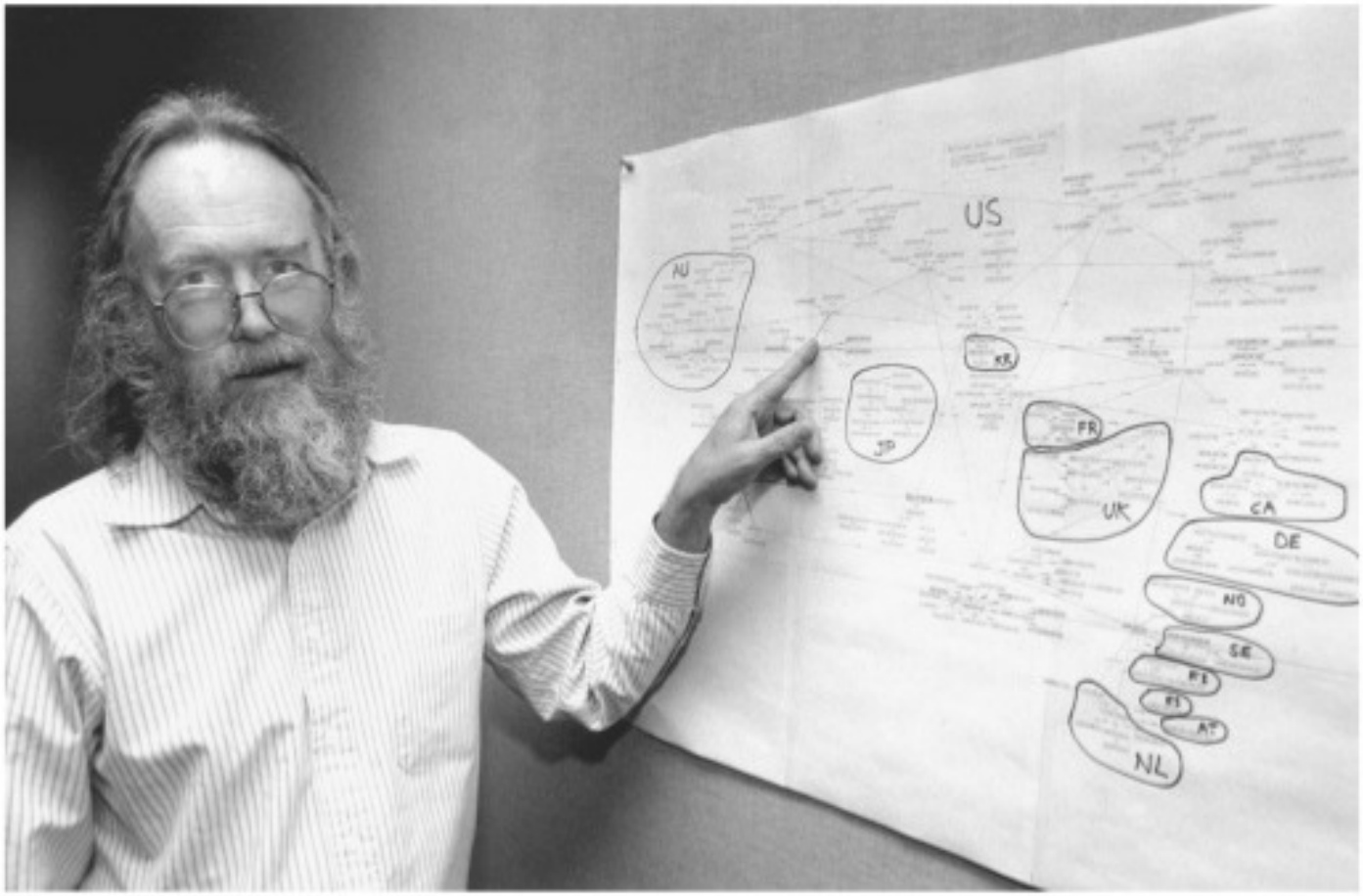
Discussion

We are screwing up in our design of internet protocols by violating the principle of layering. Specifically we are trying to use TCP to do two things: serve as a host level end to end protocol, and to serve as an internet packaging and routing protocol. These two things should be provided in a layered and modular way. I suggest that a new distinct internetwork protocol is needed, and that TCP be used strictly as a host level end to end protocol. I also believe that if TCP is used only in this cleaner way it can be simplified somewhat. A third item must be specified as well -- the interface between the internet host to host protocol and the internet hop by hop protocol.

An analogy may be drawn between the internet situation and the ARPANET. The endpoints of message transmissions are hosts in both cases, and they exchange messages conforming to a host to host protocol. In the ARPA subnet there is a IMP to IMP protocol that is primarily a hop by hop protocol, to parallel this the internet system should have a hop by hop internet protocol. In the ARPANET a host and an IMP interact through an inteface, commonly called 1822, which specifies the format of messages crossing the boundary, an equivalent interface in needed in the internet system.

Jon Postel

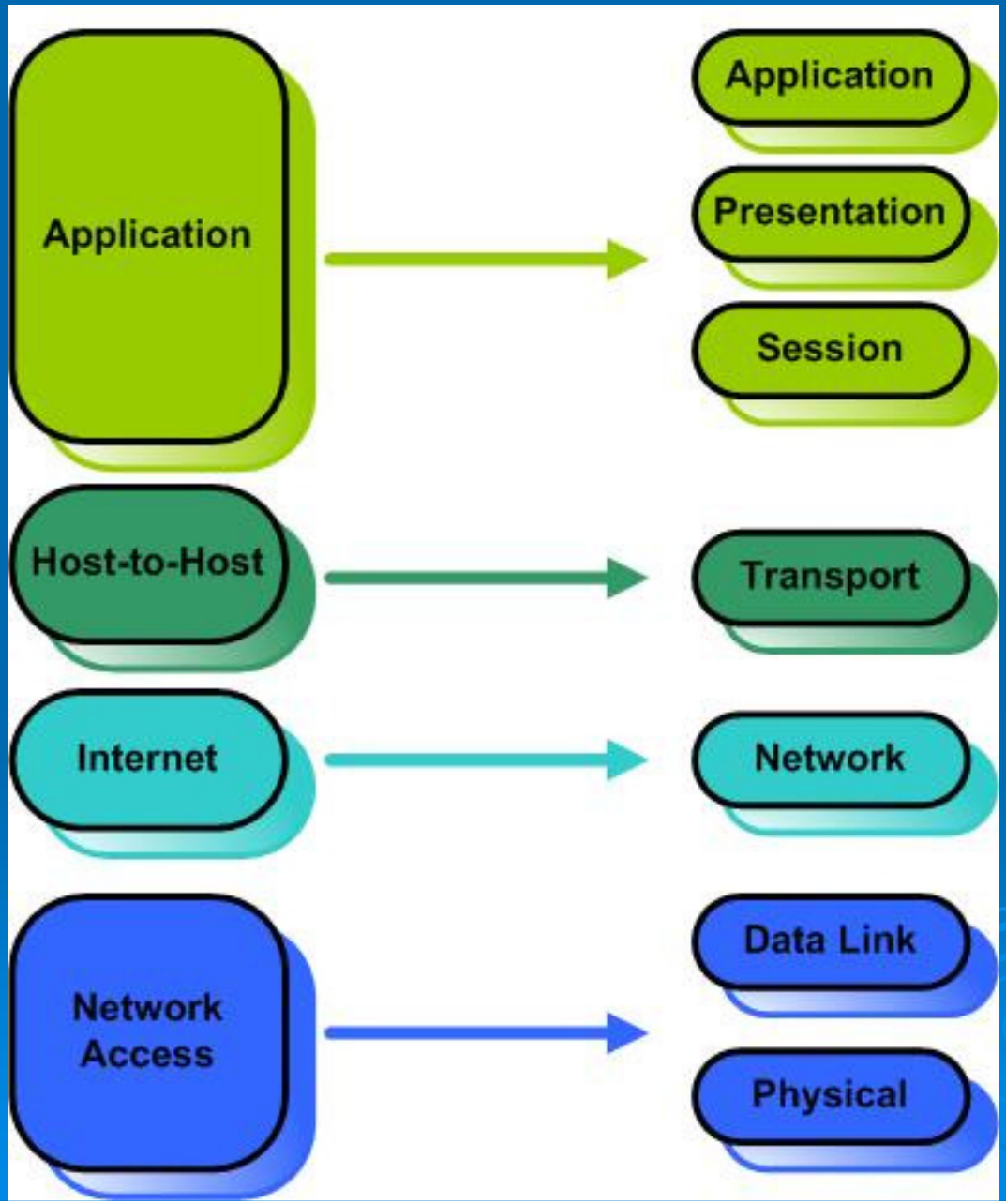
Jon Postel: The IANA Until 1998



The Internet Society

TCP/IP Model

- Not an exact mapping!
- e.g. Host-to-Host can also include some session layer

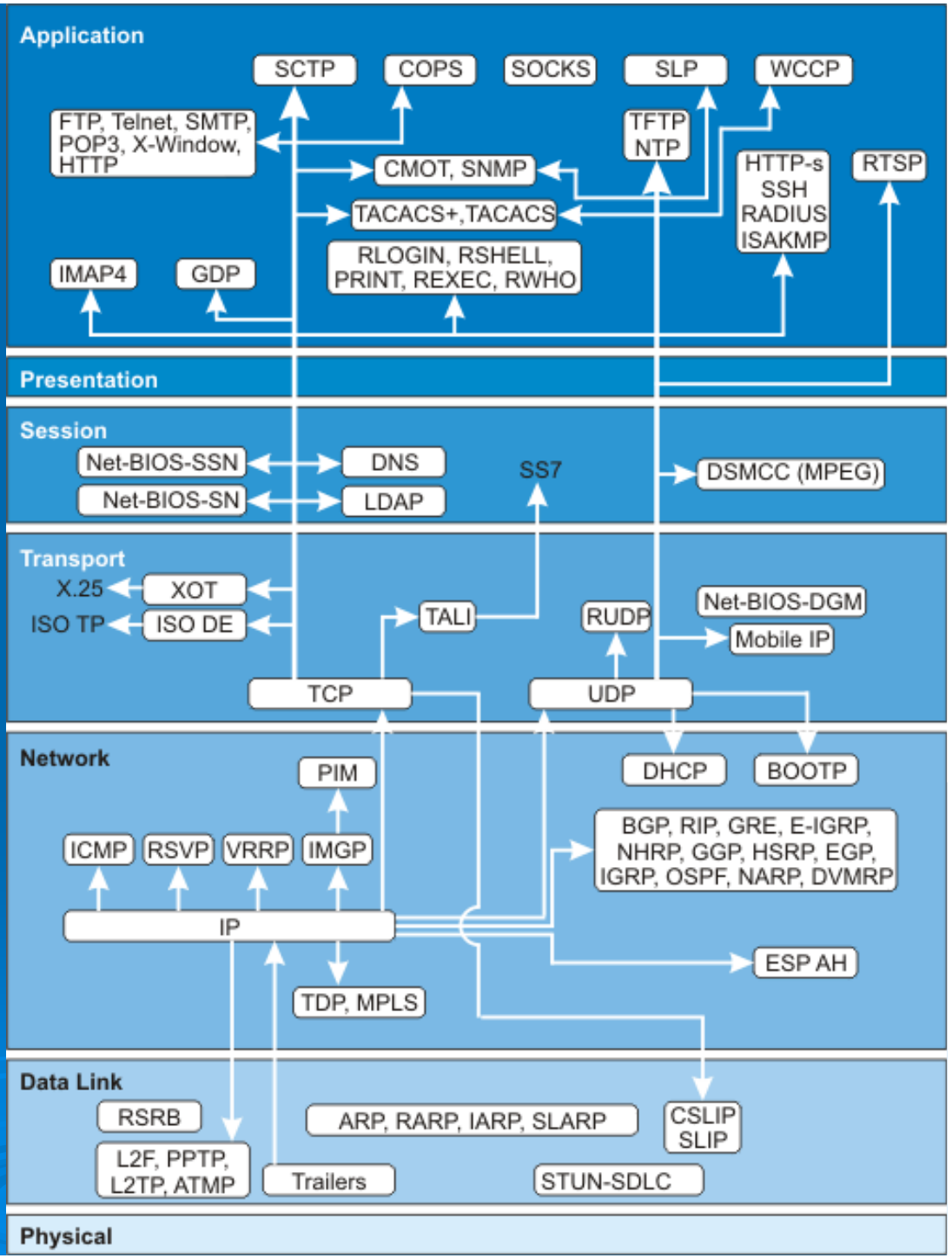


Stelios Antoniou "Networking Basics: TCP, UDP, TCP/IP & OSI models" http://www.trainsignaltraining.com/wpnew/wp-content/uploads/2007/10/TCP__OSI___Stelios/1_TCPIP_and_OSI_models.jpg

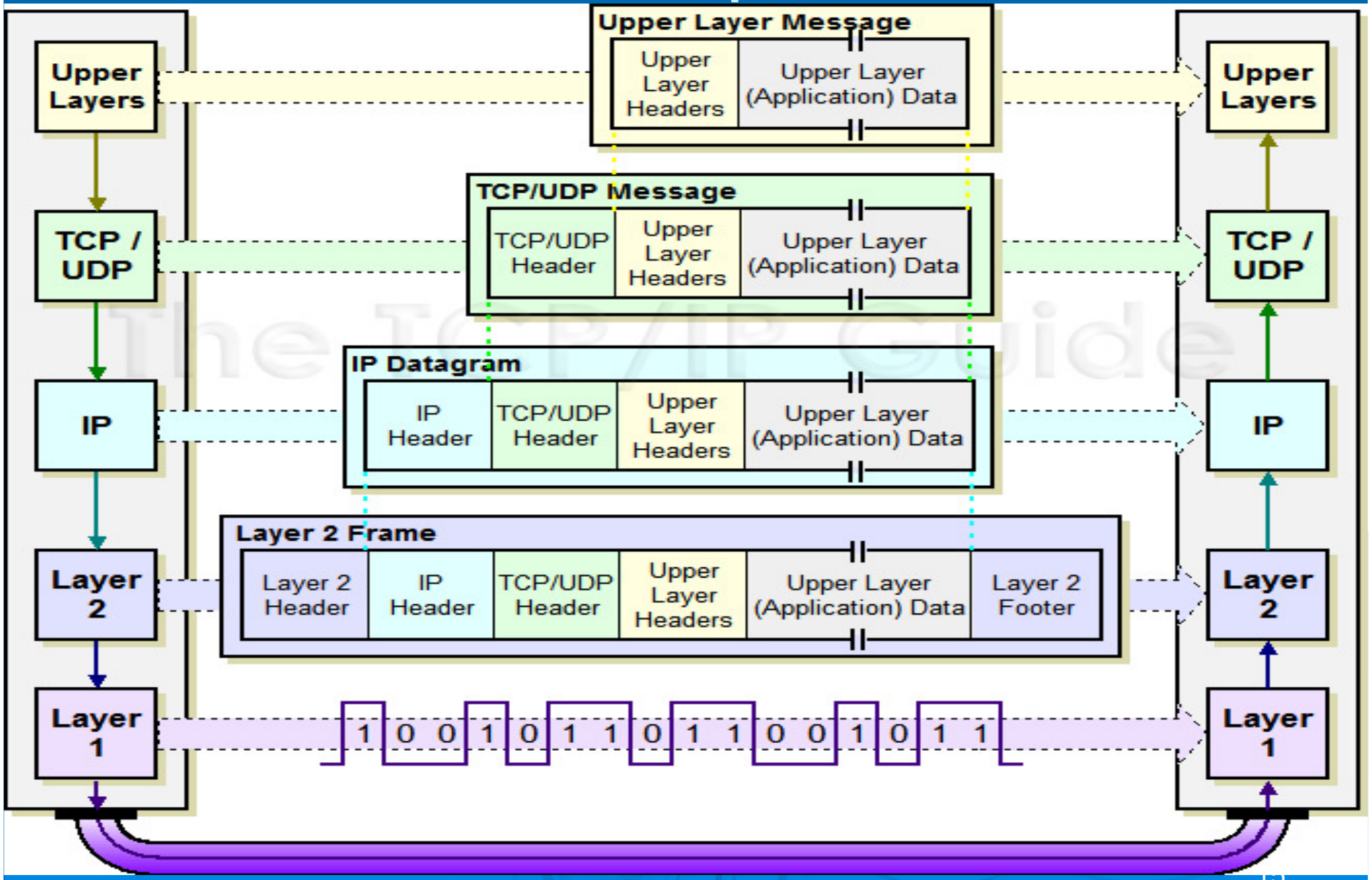
OSI Mapping

- Networking components

Protocols.com “TCP/IP Reference Page”
http://www.protocols.com/pbook/images/tcpipmap.gif

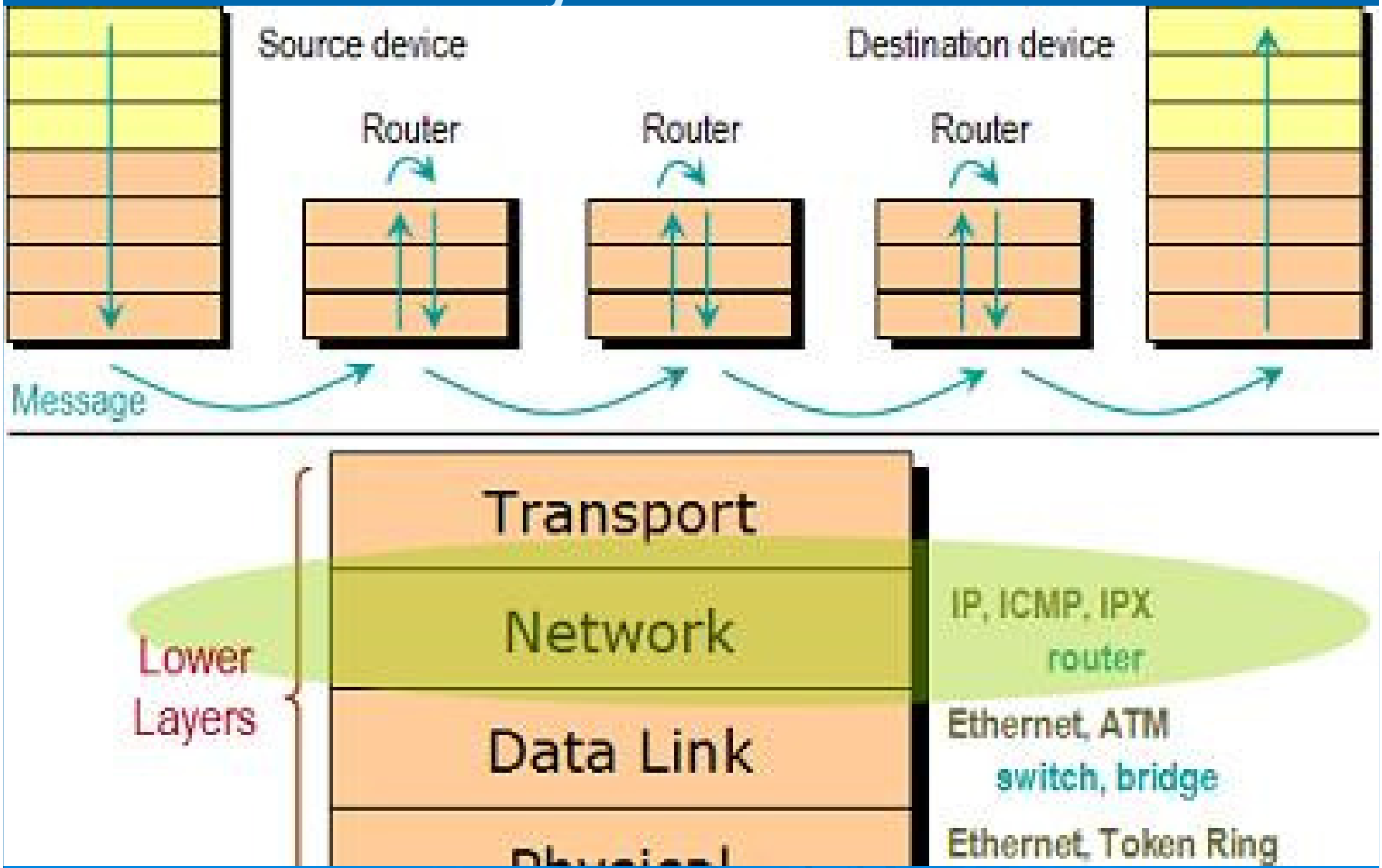


TCP/IP Encapsulation



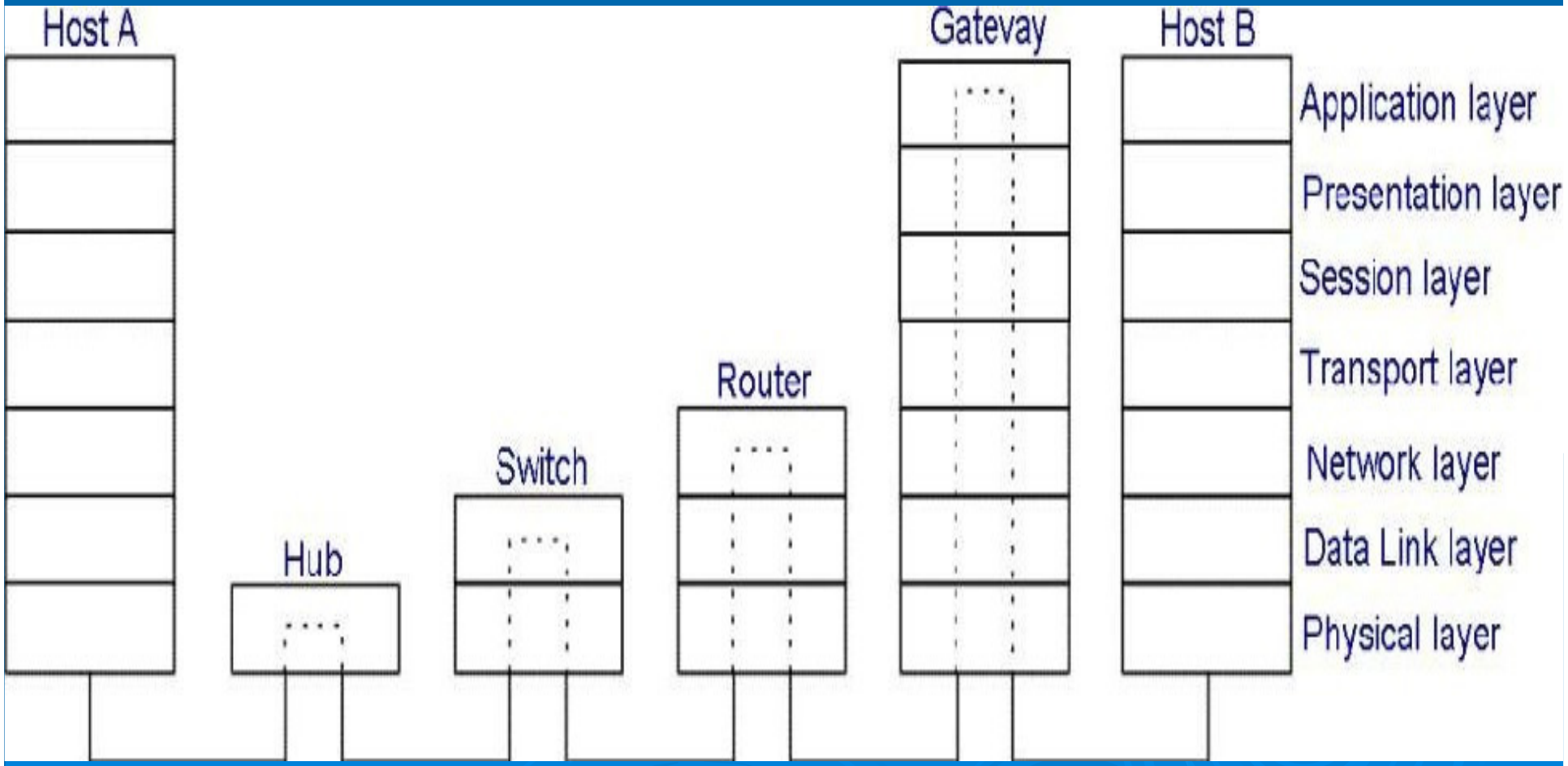
Charles M. Kozierok, "The TCP/IP Guide" http://www.tcpipguide.com/free/diagrams/ipencap.png

Network Layer Communication



Bradley Mitchell, "Visual Networking Overview - The OSI Model - Network Layer"
http://compnetworking.about.com/library/graphics/basics_osimodel_network.jpg

Actually many Layer 1,2 or 3 Devices

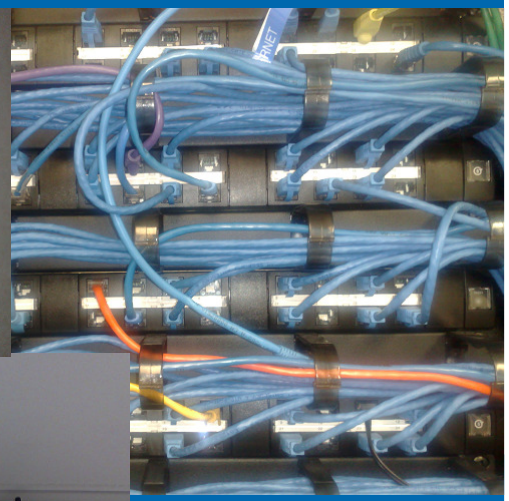


Eldis Mujarić, “Figure 13: Networking devices and OSI model” http://networking.layer-x.com/pic/fig013.jpg

Any questions so far?

Physical Layer Security

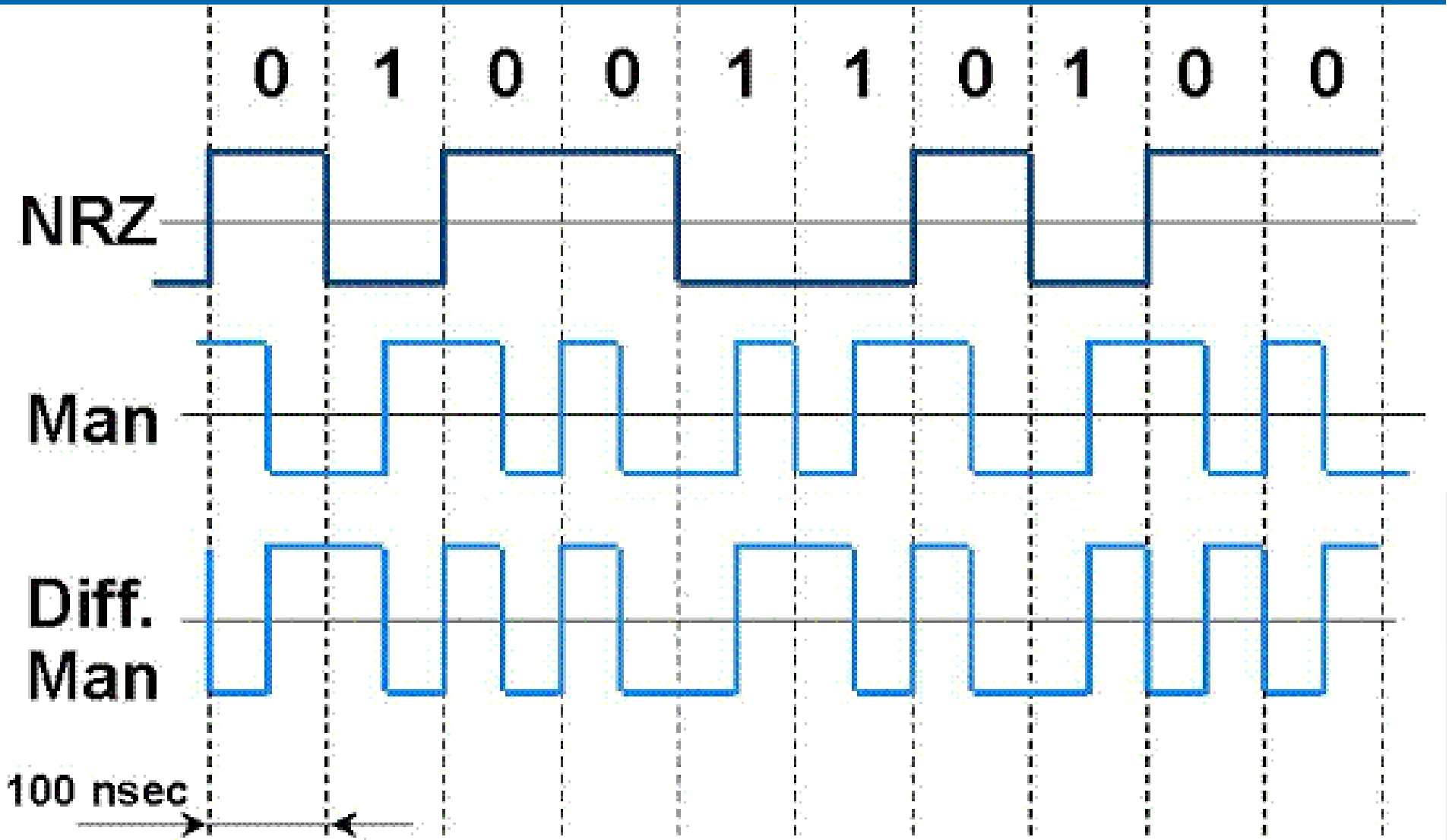
- Wired/UTP/Co-axial/Fibre
  - Access to jacks
  - Access to wires
  - Patch panels
- Wireless
  - Access to jacks (the air)
  - Access to wires (the air)
  - Patch panels (the air)



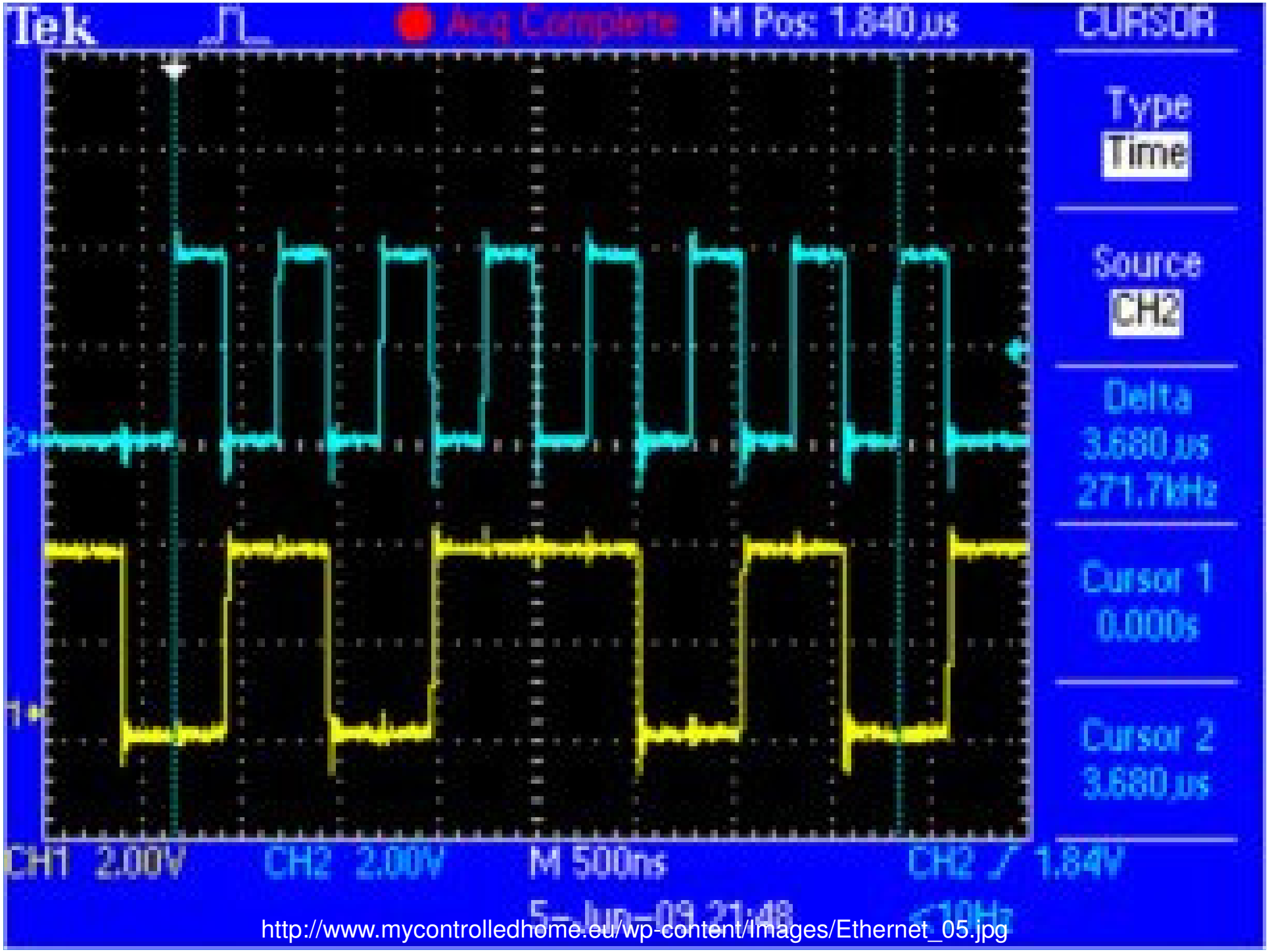
Confidentiality

- Access to the medium
- Medium accessed
  - Just volts on the wire
  - Packet sniffing
  - Promiscuous mode interfaces

Just volts over the wire

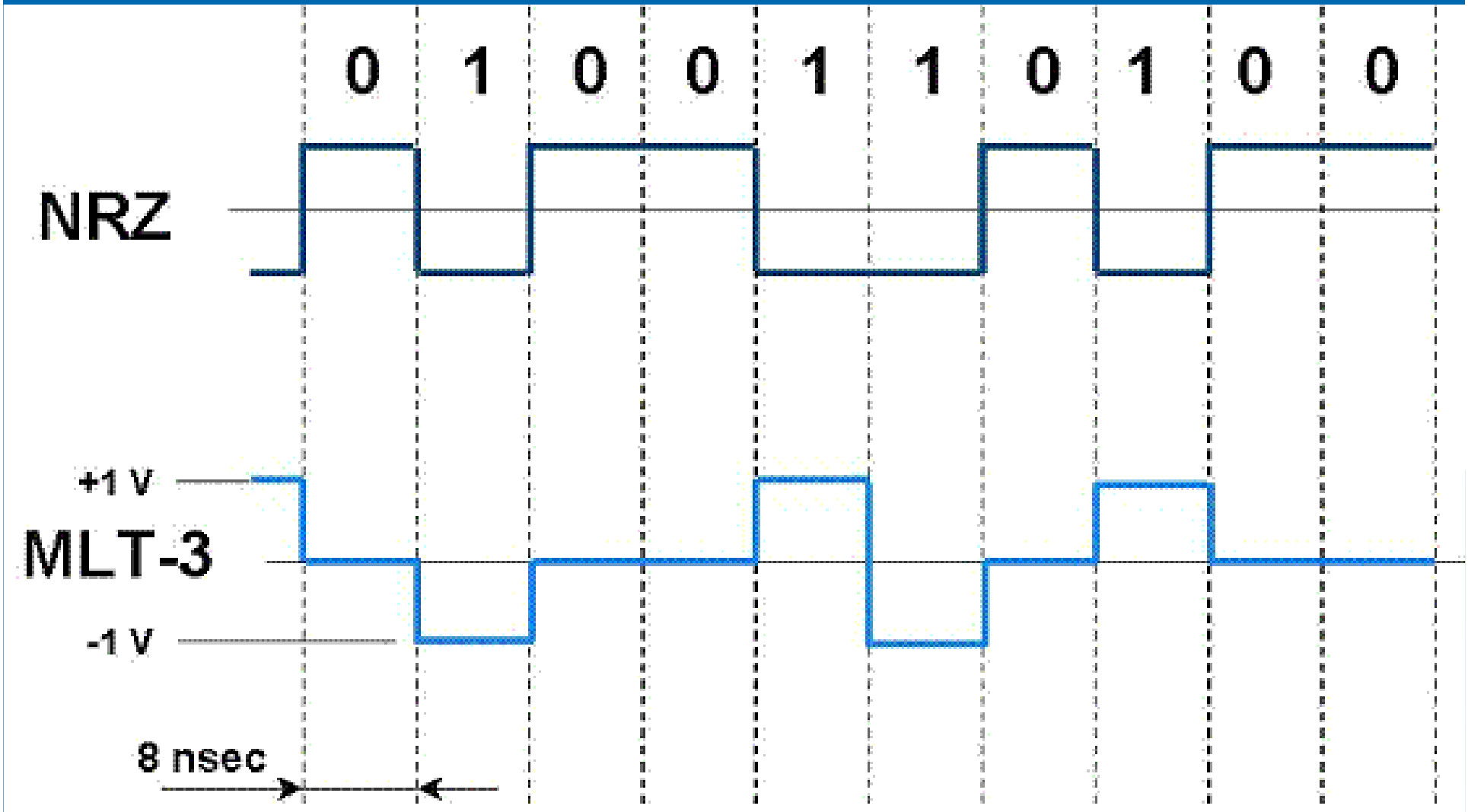


Fluke, http://www.flukenetworks.com/NR/rdonlyres/DA235221-9526-4EEB-92BC-D0966195E258/0/image005.gif



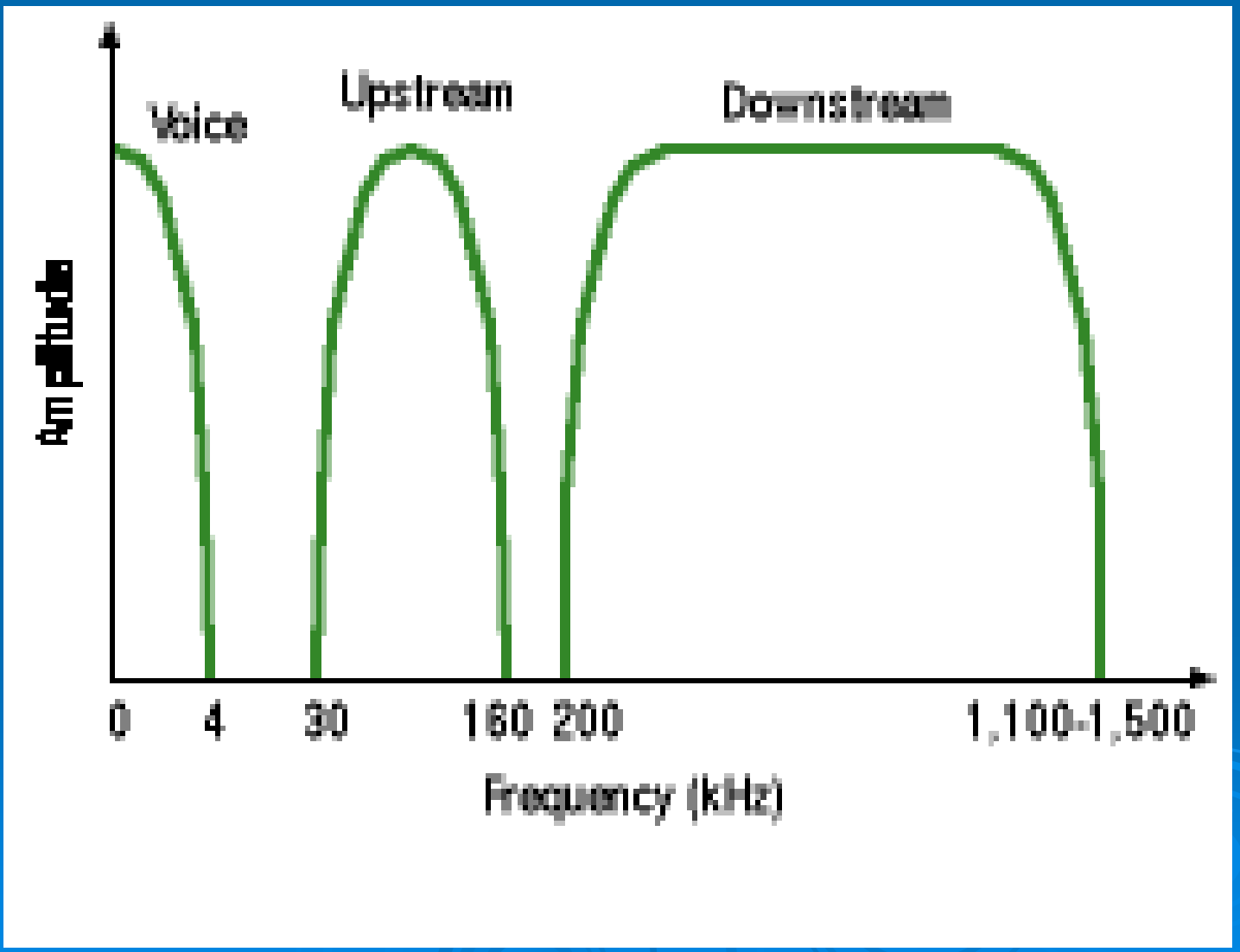
http://www.mycontrolledhome.eu/wp-content/images/Ethernet_05.jpg

It may be multi-level



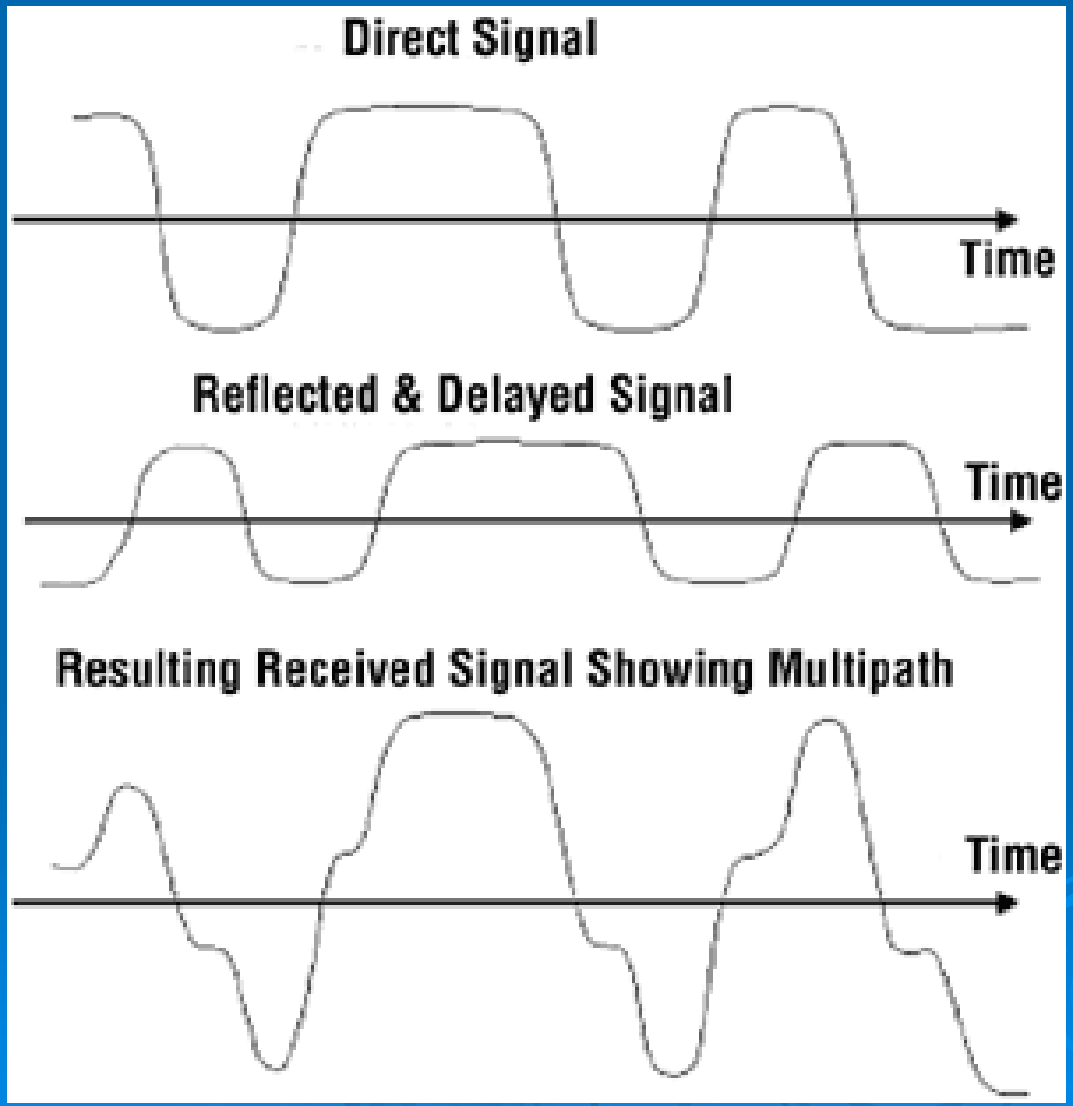
Fluke, http://www.flukenetworks.com/NR/rdonlyres/02140159-471E-4FD1-84E7-F74128338897/0/image006.gif

It may be frequency multiplexed



HAMLET ABEDMAMOORE, “ADSL”, http://www2.electronicproducts.com/images2/f11pulsd0101.gif

Integrity



Robert Lau, Peter Fuhr, “Multipath Distortion”, http://www.sensorsmag.com/files/sensor/nodes/2004/774/fig6.gif

Availability?

Geek About, “40 Most Disastrous Cable Messes”, http://img150.imageshack.us/img150/9891/30972181ne4.jpg

Data-Link Layer Security

Data-Link Layer Security

- Circuit-switched networks
  - PSTN – not any more!
- Packet-switched networks
  - IEEE 802 standards divide DLL into 2 sub-layers
    - Logical Link Control (LLC) Layer
    - Media Access Control (MAC) Layer

Media Access Control (MAC)

- Carrier Sense Multiple Access
- CSMA/Collision Avoidance (CSMA/CA)
- CSMA/Collision Detection (CSMA/CD)

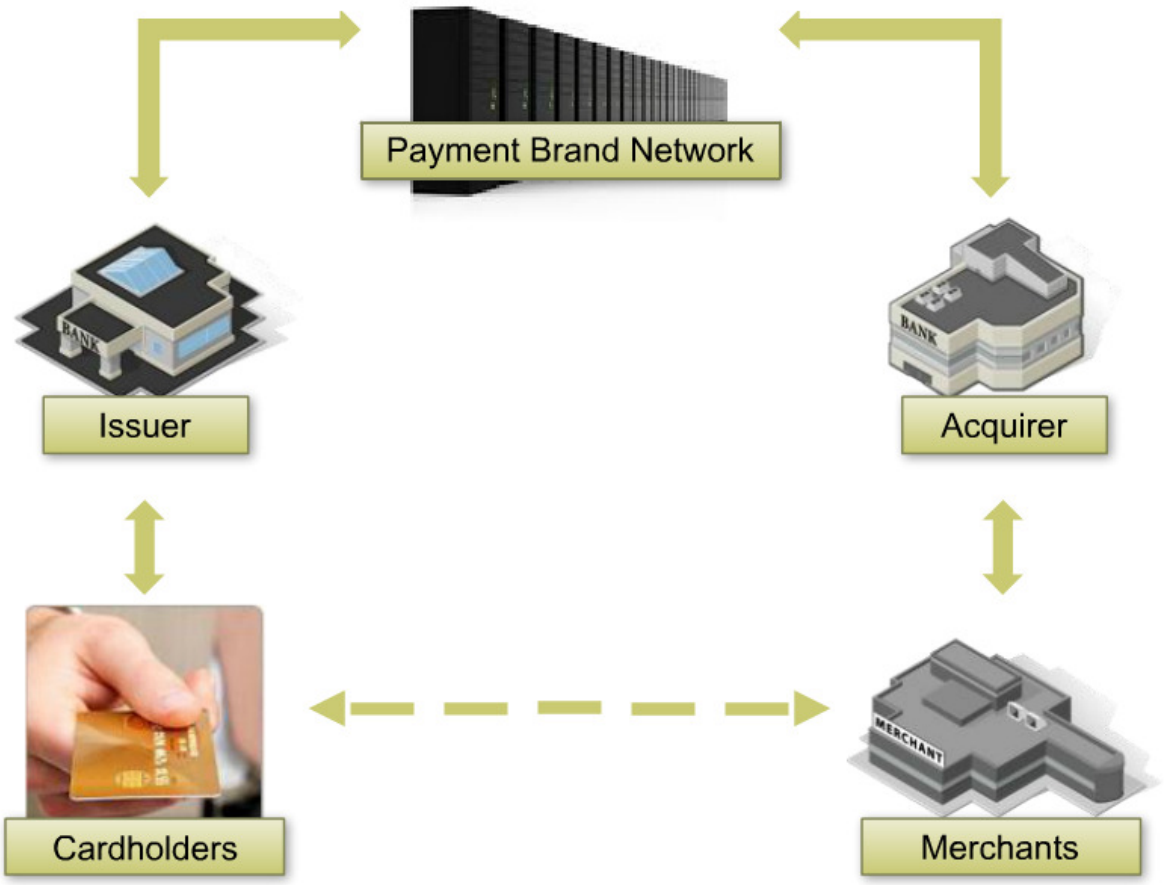
Any questions so far?

Firewalls

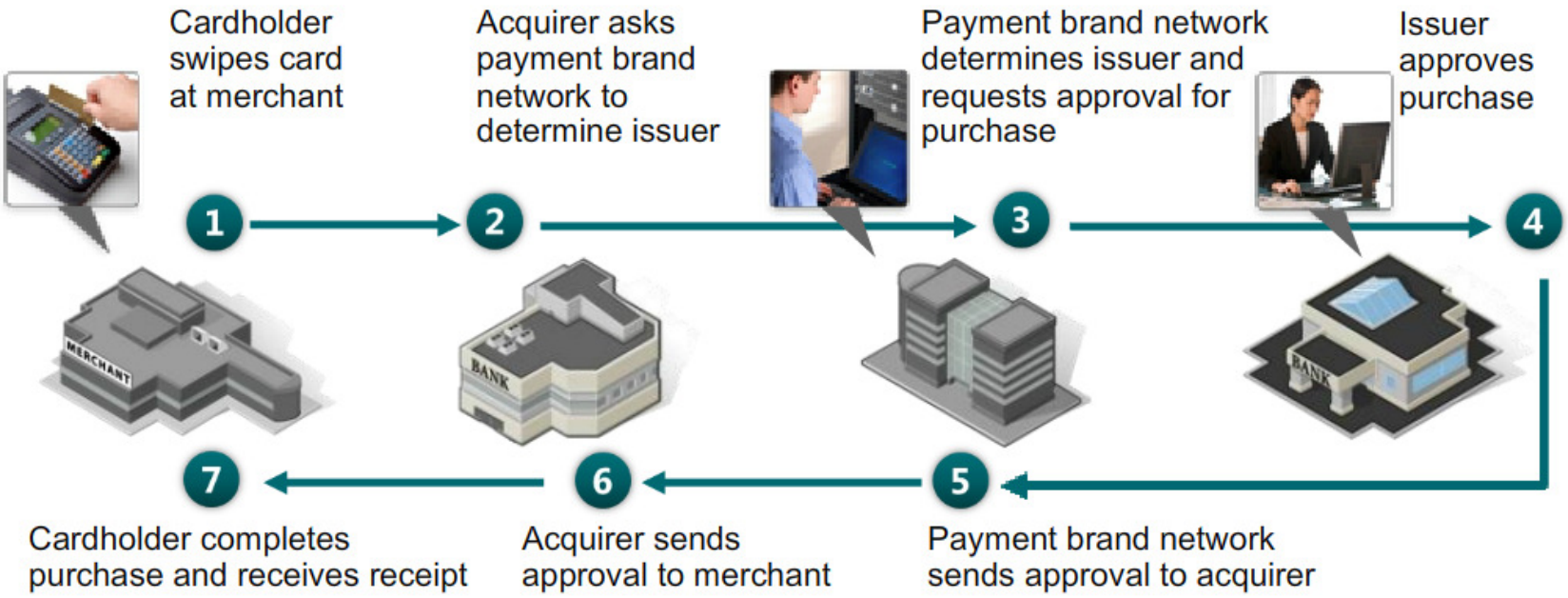
- The PCI Security Standards Council perspective:
- https://www.pcisecuritystandards.org/document_library

Payment Card Operations

Payment Industry Terminology



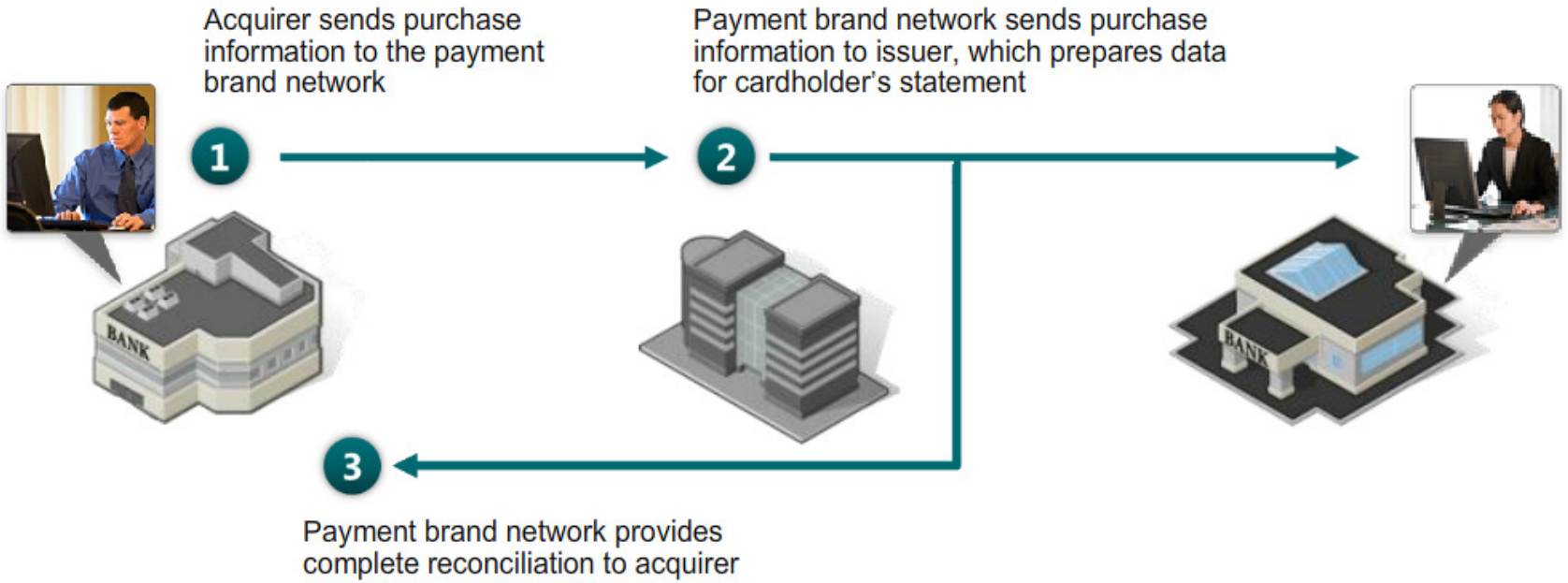
Authorisation



Authorization (Time of Purchase)

- Merchant requests and receives authorization from the Issuer to allow the purchase to be conducted.
- Authorization Code is provided.

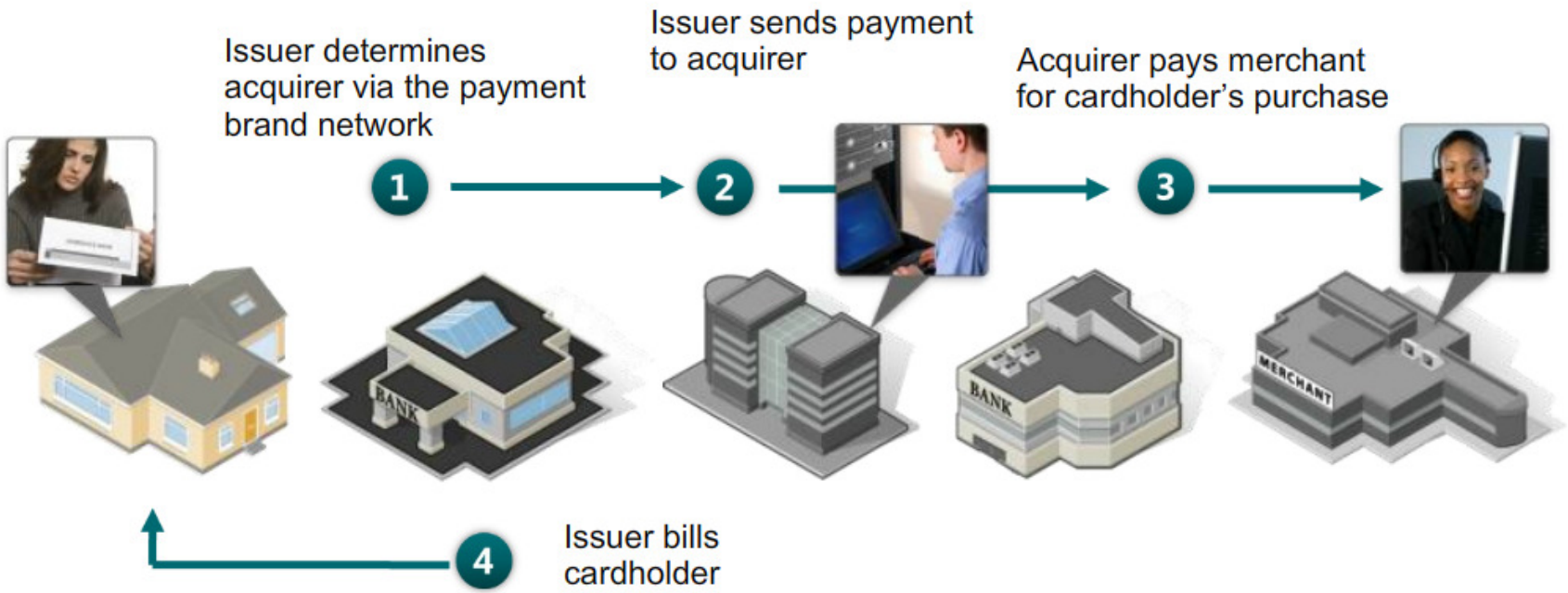
Clearing



Clearing (Usually within one day)

- Acquirer and Issuer exchange purchase information

Settlement



Settlement (Usually within two days)

- Acquirer pays merchant for cardholder purchase
- Issuer bills cardholder

PCI Data Security Standard

Six Goals, Twelve Requirements

Build and Maintain a Secure Network and Systems	1. Install and maintain a firewall configuration to protect cardholder data 2. Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	3. Protect stored cardholder data 4. Encrypt transmission of cardholder data across open, public networks
Maintain a Vulnerability Management Program	5. Protect all systems against malware and regularly update anti-virus software or programs 6. Develop and maintain secure systems and applications
Implement Strong Access Control Measures	7. Restrict access to cardholder data by business need-to-know 8. Identify and authenticate access to system components 9. Restrict physical access to cardholder data
Regularly Monitor and Test Networks	10. Track and monitor all access to network resources and cardholder data 11. Regularly test security systems and processes
Maintain an Information Security Policy	12. Maintain a policy that addresses information security for all personnel

Requirement 1 - Firewalls

- “Install and maintain a firewall configuration to protect data”
  - 1.1 Documented configuration and formal processes for firewalls and routers
  - 1.2 All external traffic and wireless traffic to pass through firewalls
  - 1.3 Implement a DMZ between Internet and Cardholder Data environment
  - 1.4 Personal firewalls on remote access PCs

Configuration Standards

1.1 Establish and implement firewall and router configuration standards that include the following:

Configuration standards and procedures will help to ensure that the organization's first line of defense in the protection of its data remains strong.

Config Standards: Approval

1.1.1 A formal process for approving and testing all network connections and changes to the firewall and router configurations

Without formal approval and testing of changes, records of the changes might not be updated, which could lead to inconsistencies between network documentation and the actual configuration.

Config Standards: Approval

PCI Security Standards Council

6. Findings and Observations

Build and Maintain a Secure Network and Systems

Requirement 1: Install and maintain a firewall configuration to protect cardholder data

PCI DSS Requirements and Testing Procedures	Reporting Instruction	ROC Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place with CCW	N/A	Not Tested	Not in Place
1.1 Establish and implement firewall and router configuration standards that include the following:							
1.1 Inspect the firewall and router configuration standards and other documentation specified below and verify that standards are complete and implemented as follows:							
1.1.1 A formal process for approving and testing all network connections and changes to the firewall and router configurations.							
1.1.1.a Examine documented procedures to verify there is a formal process for testing and approval of all: • Network connections, and • Changes to firewall and router configurations.	**Identify the document(s)** reviewed to verify procedures define the formal processes for:						
	▪ Testing and approval of all network connections.	*<Report Findings Here>*					
	▪ Testing and approval of all changes to firewall and router configurations.	*<Report Findings Here>*					
1.1.1.b For a sample of network connections, interview responsible personnel and examine records to verify that network connections were approved and tested.	▪ **Identify** the sample of records for network connections that were examined.	*<Report Findings Here>*					
	▪ **Identify** the responsible personnel interviewed who confirm that network connections were approved and tested.	*<Report Findings Here>*					
	Describe how the sampled records were examined to verify that network connections were:						
	▪ Approved	*<Report Findings Here>*					
	▪ Tested	*<Report Findings Here>*					

Config Standards: Diagrams

1.1.2 Current network diagram that identifies all connections between the cardholder data environment and other networks, including any wireless networks

Without current network diagrams, devices could be overlooked and be unknowingly left out of the security controls implemented for PCI DSS and thus be vulnerable to compromise.

Config Standards: Data Flows

1.1.3 Current diagram that shows all cardholder data flows across systems and networks

Network and cardholder data-flow diagrams help an organization to understand and keep track of the scope of their environment, by showing how cardholder data flows across networks and between individual systems and devices.

Config Standards: Firewall DMZs

1.1.4 Requirements for a firewall at each Internet connection and between any demilitarized zone (DMZ) and the internal network zone

Using a firewall on every Internet connection and between any DMZ and the internal network, allows the organization to monitor and control access and minimizes the chances of a malicious actor accessing the internal network via unprotected connection.

Standards: Roles/Responsibilities

1.1.5 Description of groups, roles, and responsibilities for management of network components

This ensures that personnel are aware of who is responsible for the security of all network components, and that those assigned to manage components are aware of their responsibilities. If roles and responsibilities are not formally assigned, devices could be left unmanaged.

Config Standards: Justify Ports

1.1.6 Documentation of business justification and approval for use of all services, protocols, and ports allowed, including documentation of security features implemented for those protocols considered to be insecure

Compromises often happen due to unused or insecure services and ports, these often have known vulnerabilities and many people don’t patch the services they don't use.

Config Standards: Justify Ports

1.1.6 …justification and approval for use of all services, protocols, and ports allowed…

- By clearly defining and documenting the services, protocols, and ports that are necessary for business, organizations can ensure that all other services, protocols, and ports are disabled or removed.
- Approvals should be granted by personnel independent of the personnel managing the configuration.

Config Standards: Justify Ports

1.1.6 …justification and approval for use of all services, protocols, and ports allowed…

- If insecure services, protocols, or ports are necessary for business, the risk should be clearly understood, the use should be justified, and the security features that allow these to be used securely should be documented and implemented. If services, protocols, or ports are not necessary, they should be disabled or removed.

Config Standards: Rule Reviews

1.1.7 Requirement to review firewall and router rule sets at least every six months

This review gives the organization an opportunity at least every six months to clean up any unneeded, outdated, or incorrect rules, and ensure that all rule sets allow only authorized services and ports that match the documented business justifications.

Restrict Connections

1.2 Build firewall and router configurations that restrict connections between untrusted networks and any system components in the cardholder data environment

It is essential to install network protection between the trusted network and any untrusted network that is external and/or out of the entity's ability to control or manage. Failure to implement this measure correctly results in the entity being vulnerable.

Restrict Connections

1.2.3 Install perimeter firewalls between all wireless networks and the cardholder data environment, and configure these firewalls to deny or, if traffic is necessary for business purposes, permit only authorized traffic between the wireless environment and the cardholder data environment.

Implement DMZs

1.3 Prohibit direct public access between the Internet and any system component in the cardholder data environment

While there may be legitimate reasons for untrusted connections to be permitted to DMZ systems (e.g., to allow public access to a web server), such connections should never be granted to systems in the internal network.

Firewall all Mobile Devices

1.4 Install personal firewall software or equivalent functionality on any portable computing devices (including company and/or employee-owned) that connect to the Internet when outside the network.

Policies and Procedures

1.5 Ensure that security policies and operational procedures for managing firewalls are documented, in use, and known to all affected parties

Personnel need to be aware of and following security policies and operational procedures to ensure firewalls and routers are continuously managed to prevent unauthorized access to the network.

Any questions so far?

IEEE 802.11 WLAN Security

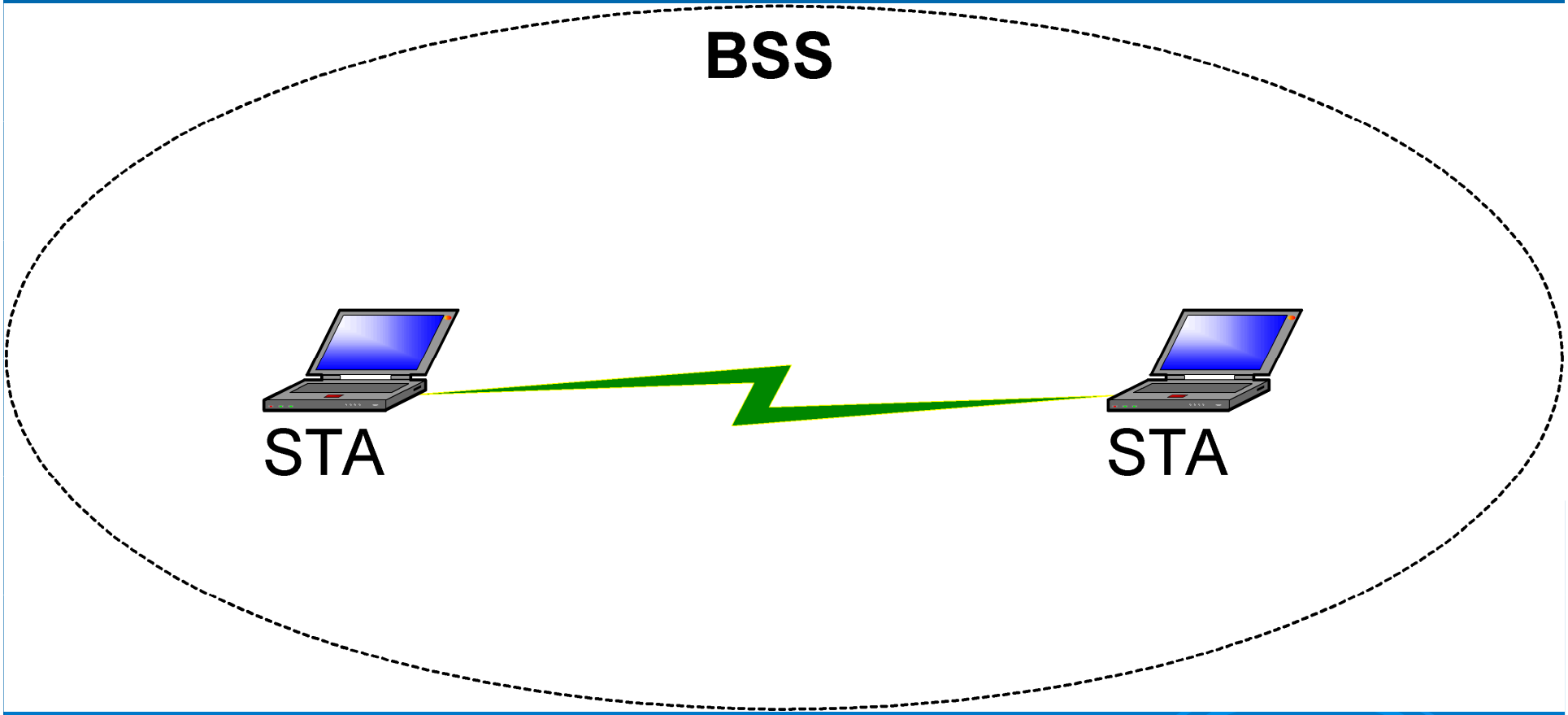
WLAN Attraction

- Allows devices to move about with freedom
- Both moveable and mobile devices
- Greater convenience than cabled networking
- Significantly reduce the time and resources needed to set up new networks
- Easy modification of networks
- Allows for networks in difficult locations
- Allows for ad hoc networks, easily created, modified or torn-down.

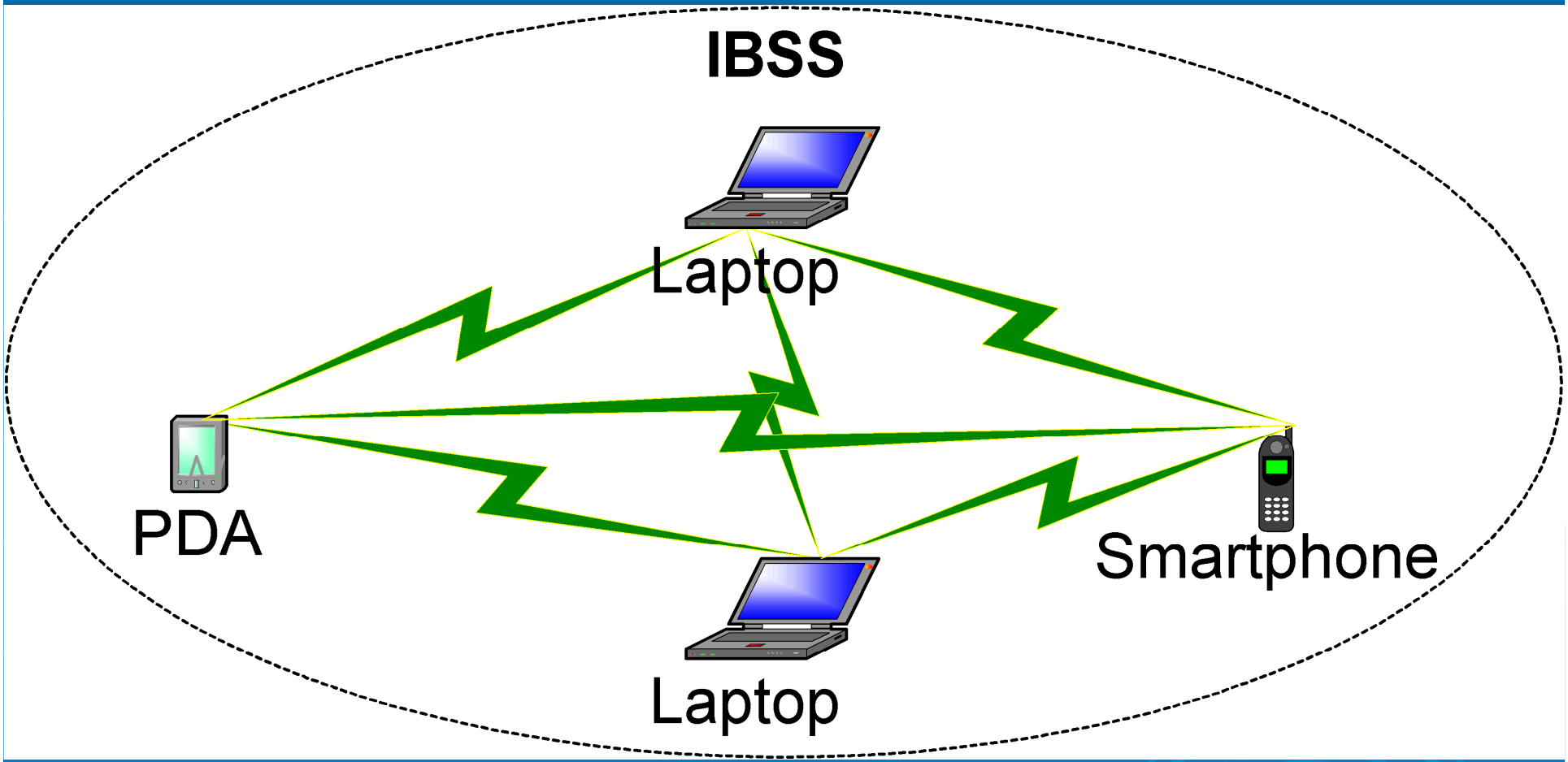
WLAN Characteristics

- IEEE 802.11 WLAN inherent characteristics
- Electromagnetic broadcast technology
- You are transmitting to the universe
- Compromise **confidentiality**
- Fragile **availability**
- Threaten **integrity**

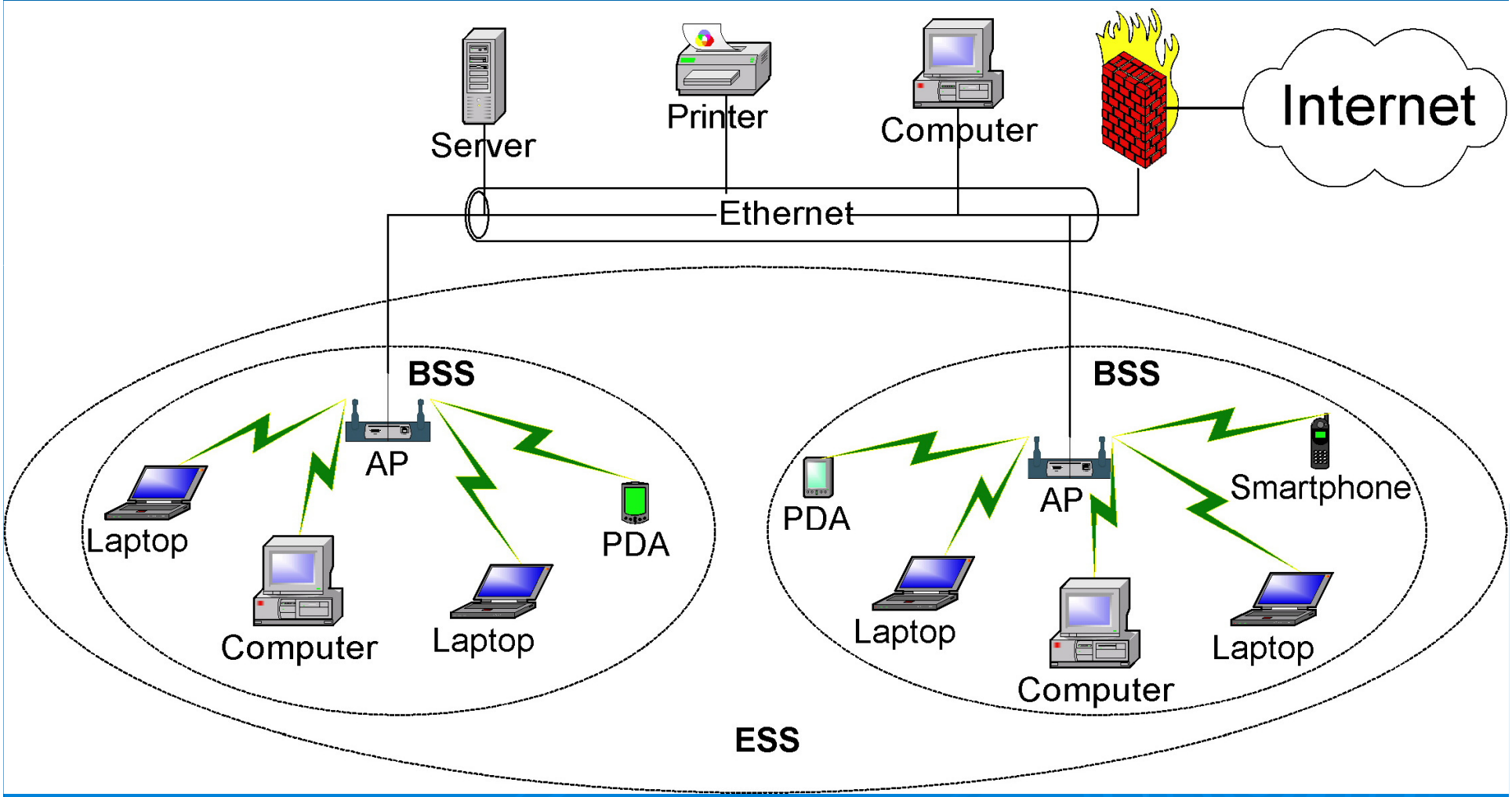
Basic Service Set (BSS)



Independent Basic Service Set (IBSS)



Extended Service Set (ESS)



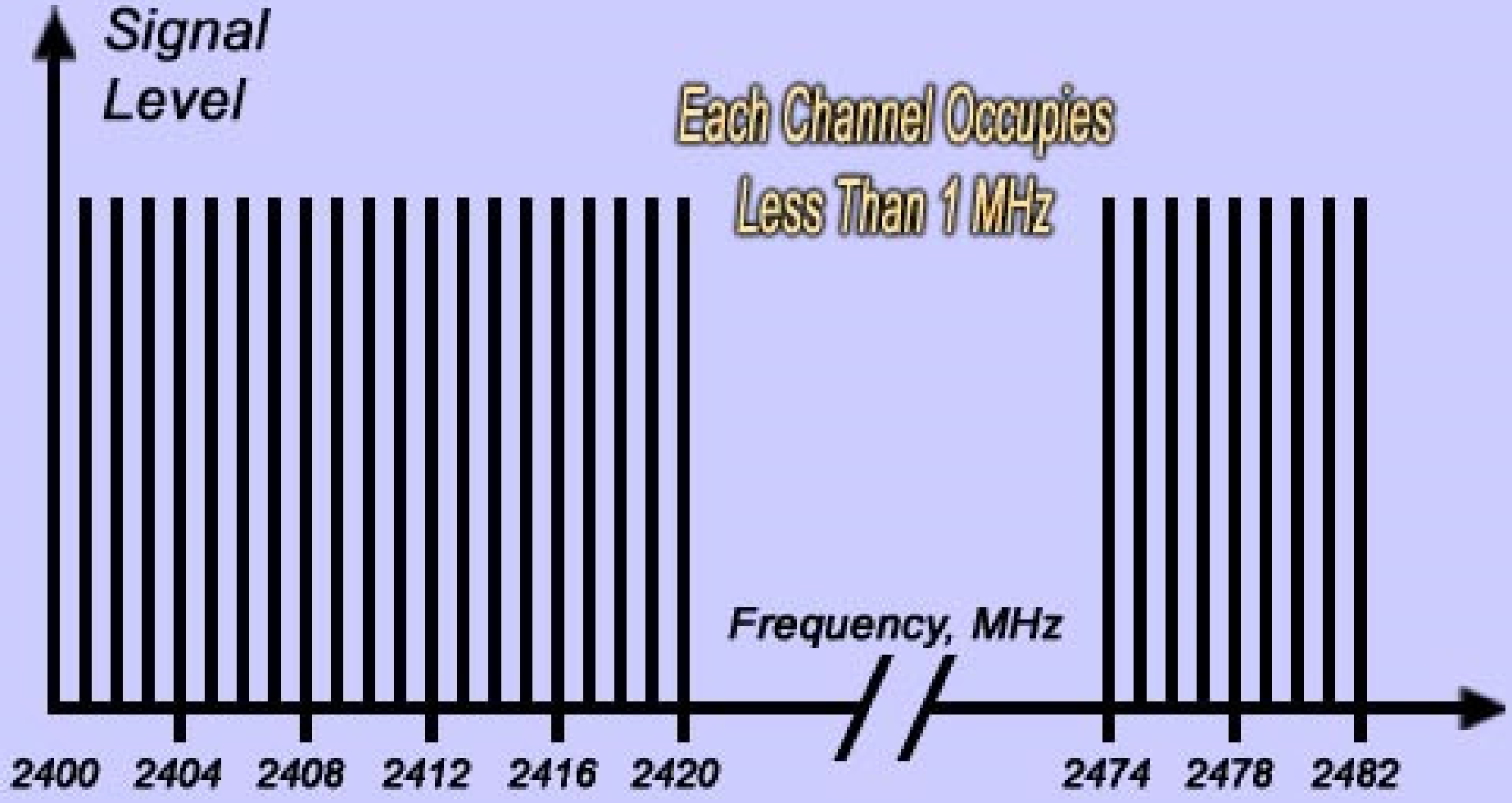
IEEE 802.11

- Two physical interfaces:
- Infra-red:
  - Up to 2 Mbps in the terahertz range
- Radio:
  - Up to 2 Mbps FHSS in 2.4 GHz band
  - Industrial, Scientific and Medical (ISM) bands
    - 2.400–2.500 GHz

IEEE 802.11 WLAN Standards

- 802.11 – Up to 2 Mbps FHSS in 2.4 GHz band
- 802.11a – Up to 54 Mbps OFDM in 5 GHz band
- 802.11b – Up to 11 Mbps DSSS in 2.4 GHz band
- TGc – Provided required information for bridge operations
- 802.11d – Additional regulatory domains (roaming)
- 802.11e – Quality of Service (QoS)
- 802.11F – RP for AP Interoperability (withdrawn)
- 802.11g – Up to 54 Mbps in the 2.4GHz band
  OFDM above 20Mbps, DSSS below 20Mbps
- 802.11h – Spectrum & Power Mgt in 5 GHz band

FHSS



(WiFi Tech Fundamentals) from http://www.wirelessnetworkproducts.com/images/tech_fund_fhss.jpg

DSSS

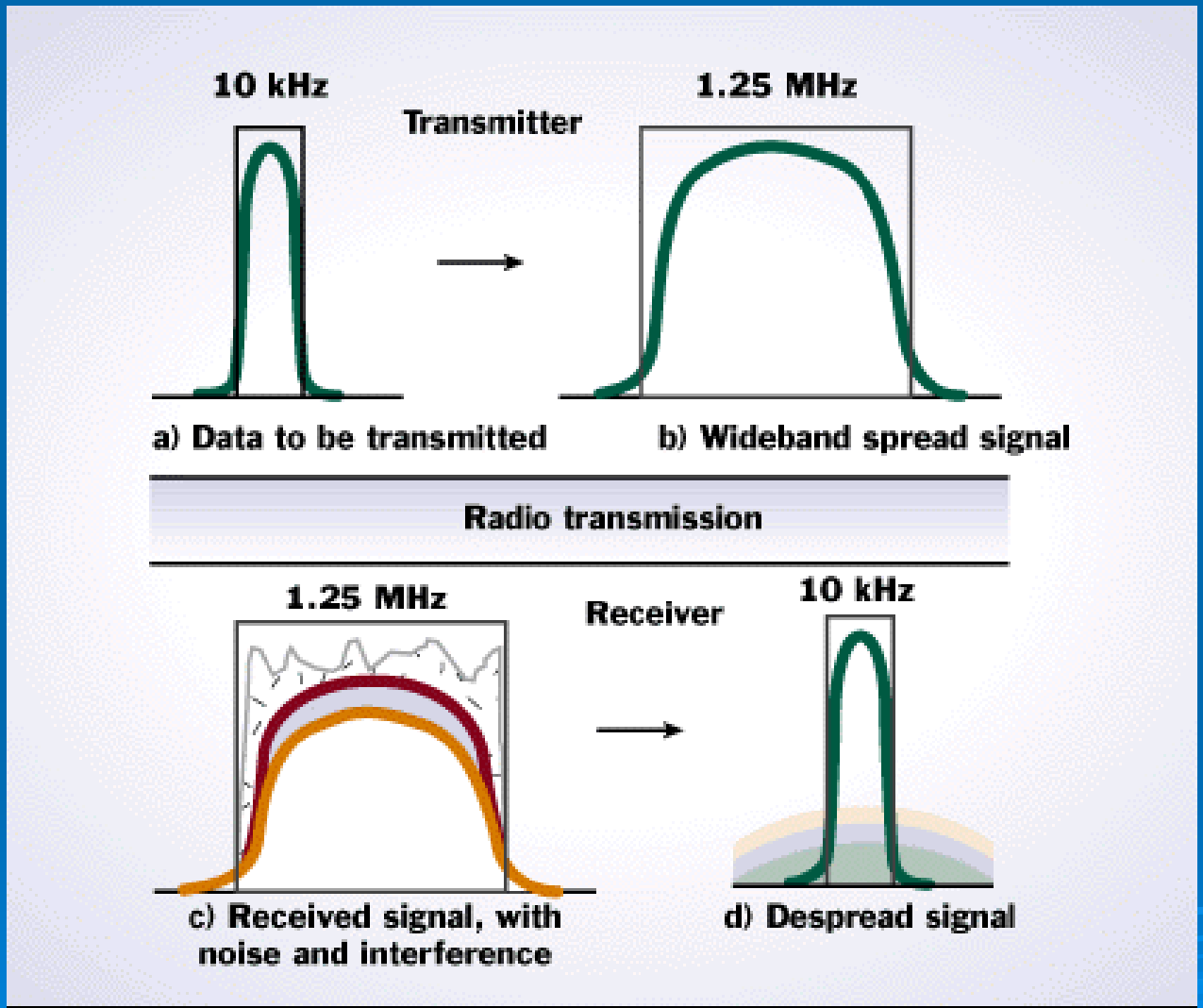
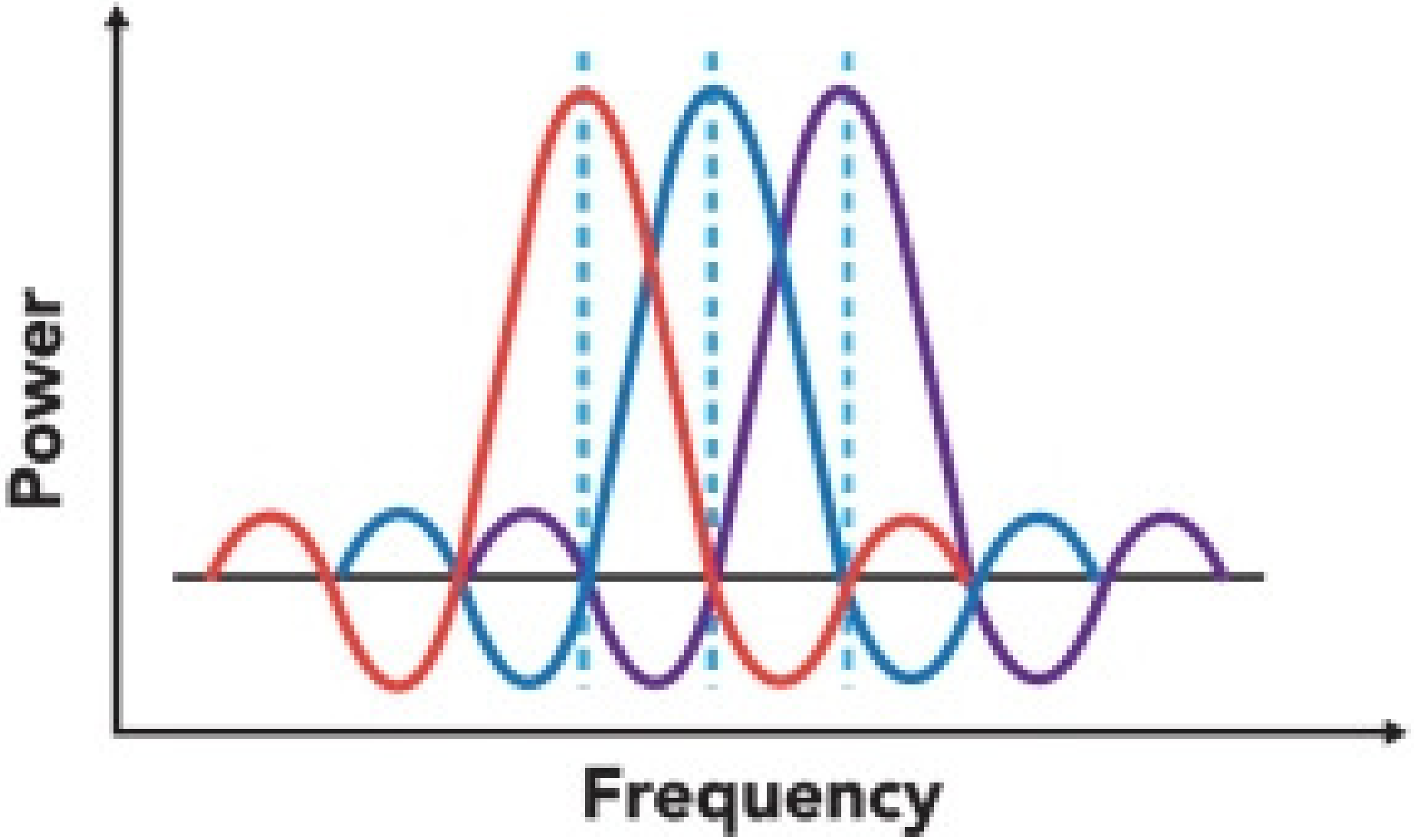


FIGURE 1: *Illustration of the DSSS data transmission technique popular in many WLAN architectures.*

James C. Chen, “EE Times” from http://i.cmpnet.com/csd/gifs/2001/02/0201ieee1.gif

OFDM



ProSoft Technology Inc , “OFDM waveform with subcarriers” from
http://www.processonline.com.au/uploads/Image/1001Feat1-2-OFDM.jpg

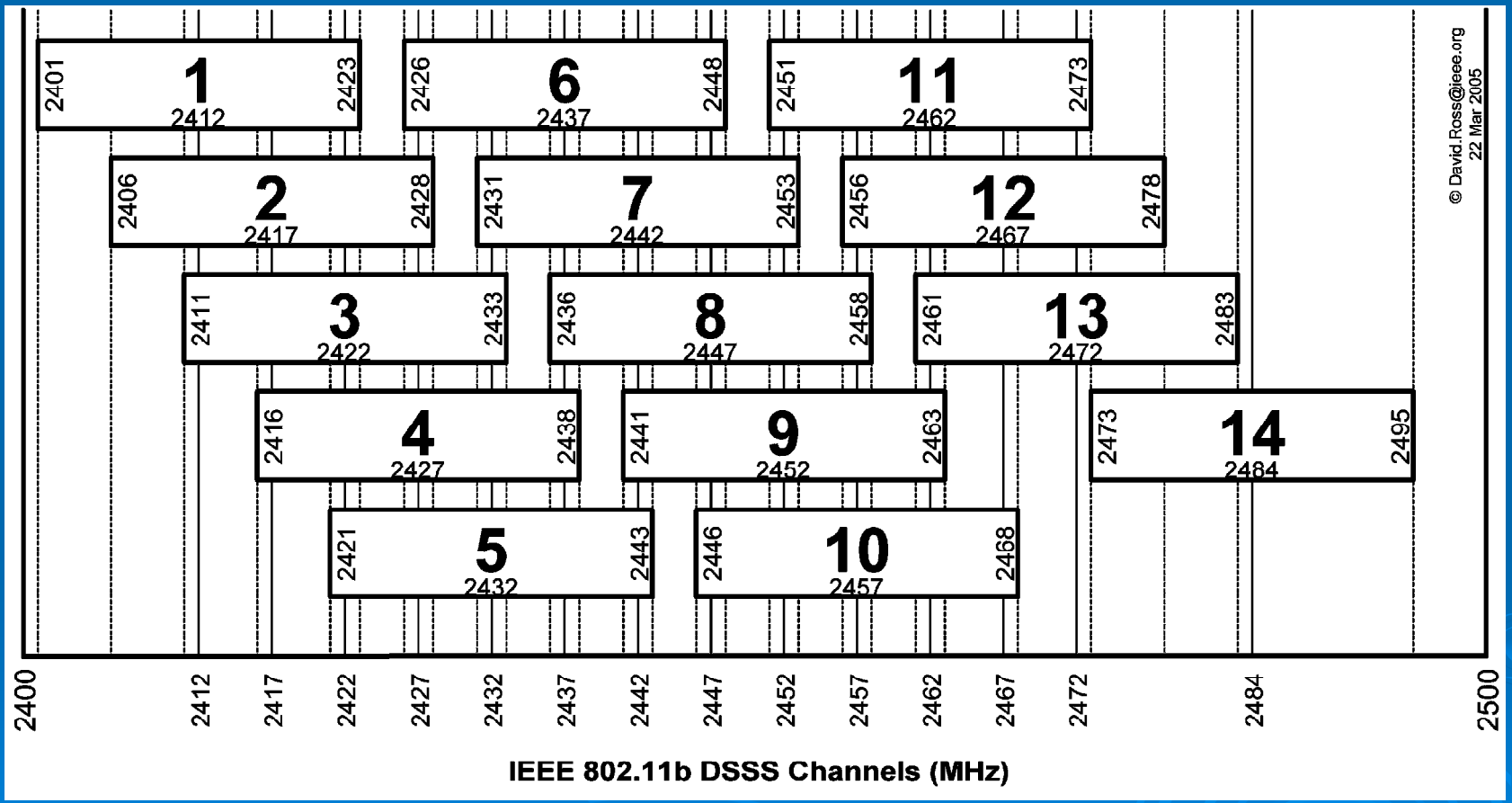
IEEE 802.11a OFDM Channels

- 3 bands, but only one is international ISM
- 2 lower bands are USA specific UNII
  - (Unlicensed National Information Infrastructure)
  - 5.2 GHz band (5150-5350 MHz)
  - In Australia, these can be used under the Low Interference Potential Devices Class Licence
- Upper band is 5.8 GHz (5725-5825 MHz) ISM

IEEE 802.11a OFDM Channels

- USA UNII Lower Band – 36, 40, 44, 48
- USA UNII Middle Band – 52, 56, 60, 64
- USA UNII Upper Band
  (ISM 5.8 GHz Band) – 149, 153, 157, 161

IEEE 802.11b DSSS Channels



Wi-Fi® Alliance Wi-Fi CERTIFIED™

Originally – 3Com, Aironet (now Cisco), Harris Semiconductor (now Intersil), Lucent (now Agere), Symbol Technologies (now Motorola), Sony, Apple, and Panasonic formed the Wireless Ethernet Compatibility Alliance (WECA) to promote 802.11b and branded the technology ***Wi-Fi***

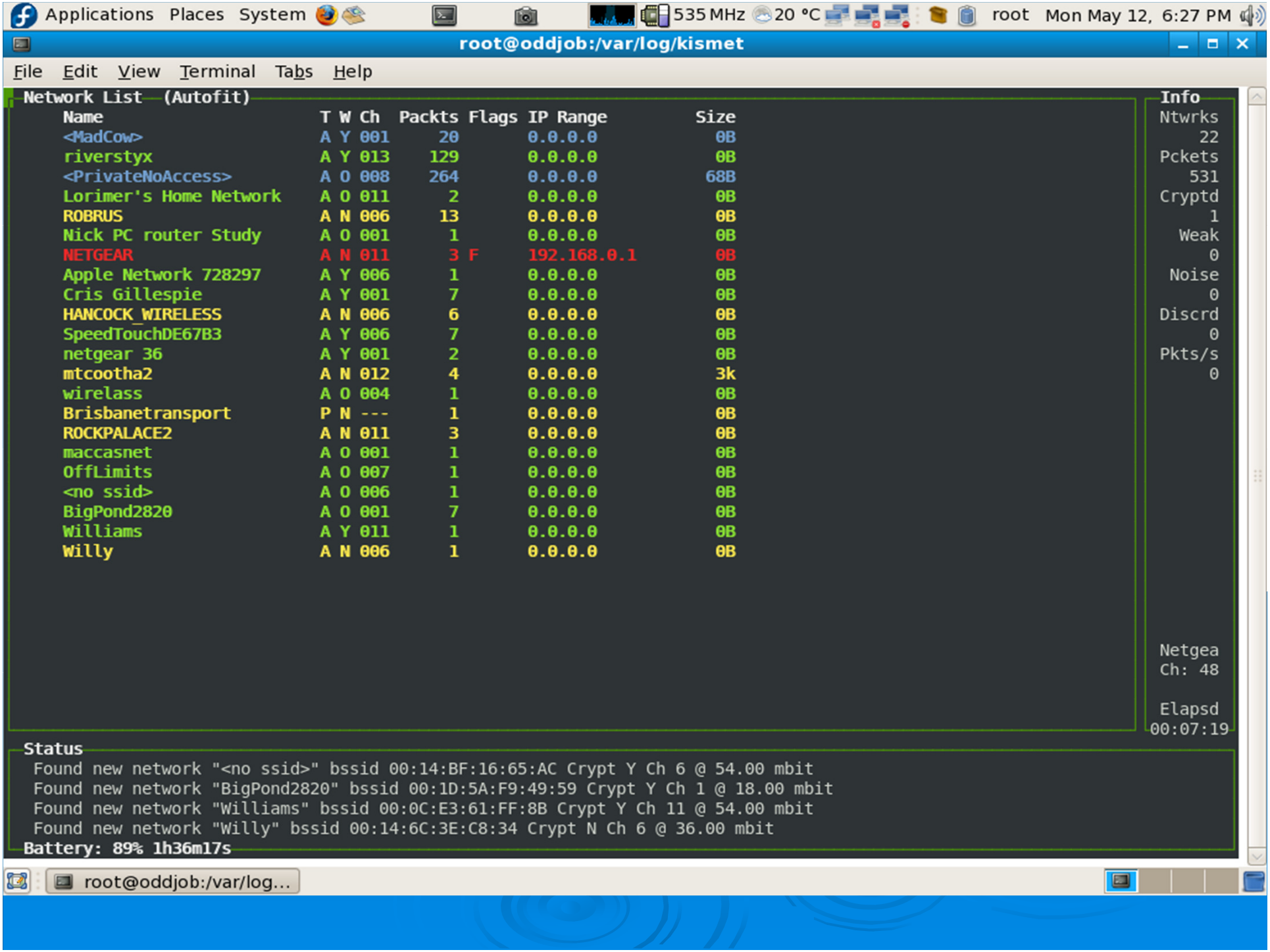
Any questions so far?

WLAN Threats

- Eavesdropping (loss of confidentiality)
- Masquerading and Resource Theft
- Traffic Redirection
  - Eavesdropping (confidentiality)
  - Tampering (integrity)
- Denial of Service (DoS)
  - General DoS
  - Stealth DoS

WLAN Security

- Service Set Identifier (SSID)
- MAC-address authentication
- Wired Equivalent Privacy (WEP)
  - One-way Authentication
  - Static WEP Keys
  - Key Size
  - Initialization Vector (IV)


Applications Places System
535 MHz 20 °C root Mon May 12, 6:27 PM
root@oddjob:/var/log/kismet
File Edit View Terminal Tabs Help
Network List (Autofit)
Name T W Ch Packts Flags IP Range Size
<MadCow> A Y 001 20 0.0.0.0 0B
riverstyx A Y 013 129 0.0.0.0 0B
<PrivateNoAccess> A O 008 264 0.0.0.0 68B
Lorimer's Home Network A O 011 2 0.0.0.0 0B
ROBRUS A N 006 13 0.0.0.0 0B
Nick PC router Study A O 001 1 0.0.0.0 0B
NETGEAR A N 011 3 F 192.168.0.1 0B
Apple Network 728297 A Y 006 1 0.0.0.0 0B
Cris Gillespie A Y 001 7 0.0.0.0 0B
HANCOCK_WIRELESS A N 006 6 0.0.0.0 0B
SpeedTouchDE67B3 A Y 006 7 0.0.0.0 0B
netgear 36 A Y 001 2 0.0.0.0 0B
mtcootha2 A N 012 4 0.0.0.0 3k
wirelass A O 004 1 0.0.0.0 0B
Brisbanetransport P N --- 1 0.0.0.0 0B
ROCKPALACE2 A N 011 3 0.0.0.0 0B
maccasnet A O 001 1 0.0.0.0 0B
OffLimits A O 007 1 0.0.0.0 0B
<no ssid> A O 006 1 0.0.0.0 0B
BigPond2820 A O 001 7 0.0.0.0 0B
Williams A Y 011 1 0.0.0.0 0B
Willy A N 006 1 0.0.0.0 0B
Info
Ntwrks 22
Pckets 531
Cryptd 1
Weak 0
Noise 0
Discrd 0
Pkts/s 0
Netgea
Ch: 48
Elapsd
00:07:19
Status
Found new network "<no ssid>" bssid 00:14:BF:16:65:AC Crypt Y Ch 6 @ 54.00 mbit
Found new network "BigPond2820" bssid 00:1D:5A:F9:49:59 Crypt Y Ch 1 @ 18.00 mbit
Found new network "Williams" bssid 00:0C:E3:61:FF:8B Crypt Y Ch 11 @ 54.00 mbit
Found new network "Willy" bssid 00:14:6C:3E:C8:34 Crypt N Ch 6 @ 36.00 mbit
Battery: 89% 1h36m17s
root@oddjob:/var/log...

WLAN Deployments

- A drive through any Brisbane suburbs:
  - Minimum 2 APs out-of-the-box factory defaults
    - Completely open
    - What do they do when someone sets the password?
  - Many SSID “Wireless” “NETGEAR” or “default”
  - Various SSID like “ICU” or “SittingDuck”
  - Some SSID are actual physical street address
  - One SSID “<no ssid>” (from David Conran’s work)

Wired Equivalent Privacy (WEP)

- Part of IEEE 802.11
- Short keys:
  - 40-bit (64-bit RC4) 40 bits secret, 24-bit cleartext IV
  - 104-bit (128-bit RC4) 104 bits secret, 24-bit cleartext IV
- Static keys + short IVs = repeated keystream
- Scott Fluhrer, Itsik Mantin & Adi Shamir – weak IVs
- Adam Stubblefield, John Ioannidis and Aviel Rubin

FMS WEP Attacks

- Quickly incorporated into tools like **AirSnort**
- 5-10 million encrypted packets
- Less than 1 second
- Vendors removed weakest IVs from new implementations
- Various enhanced-FMS attacks

Statistical WEP Attacks

- **KoreK** posted new WEP statistical cryptanalysis attack code to the NetStumbler forums 08/08/04
- The attacks do not require millions of packets
- The number of weak IVs does not matter
- Need hundreds of thousands of unique IVs
- Incorporated into tools like **aircrack** & **WepLab**
- WEP thoroughly broken

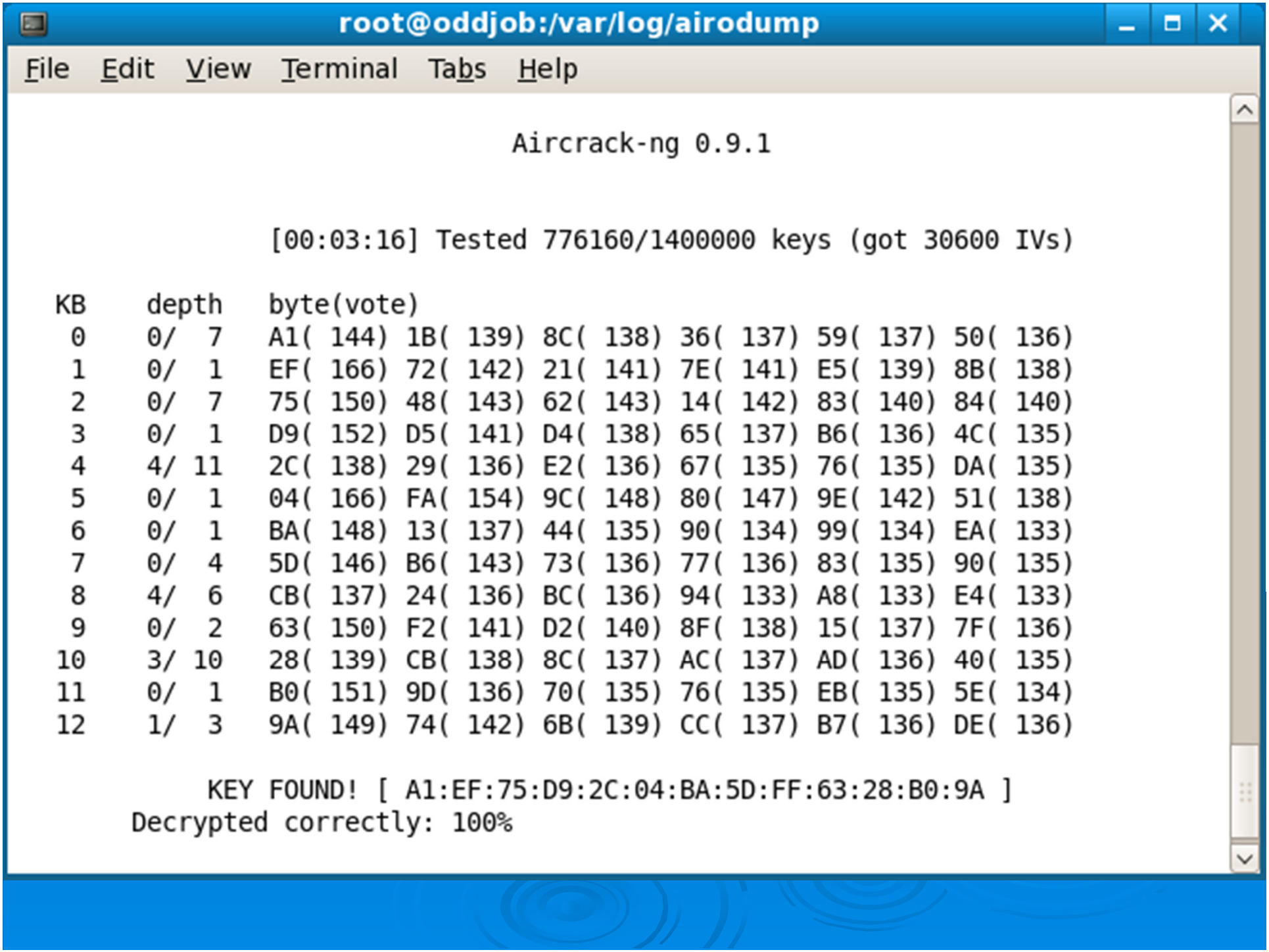
aircrack 2.0

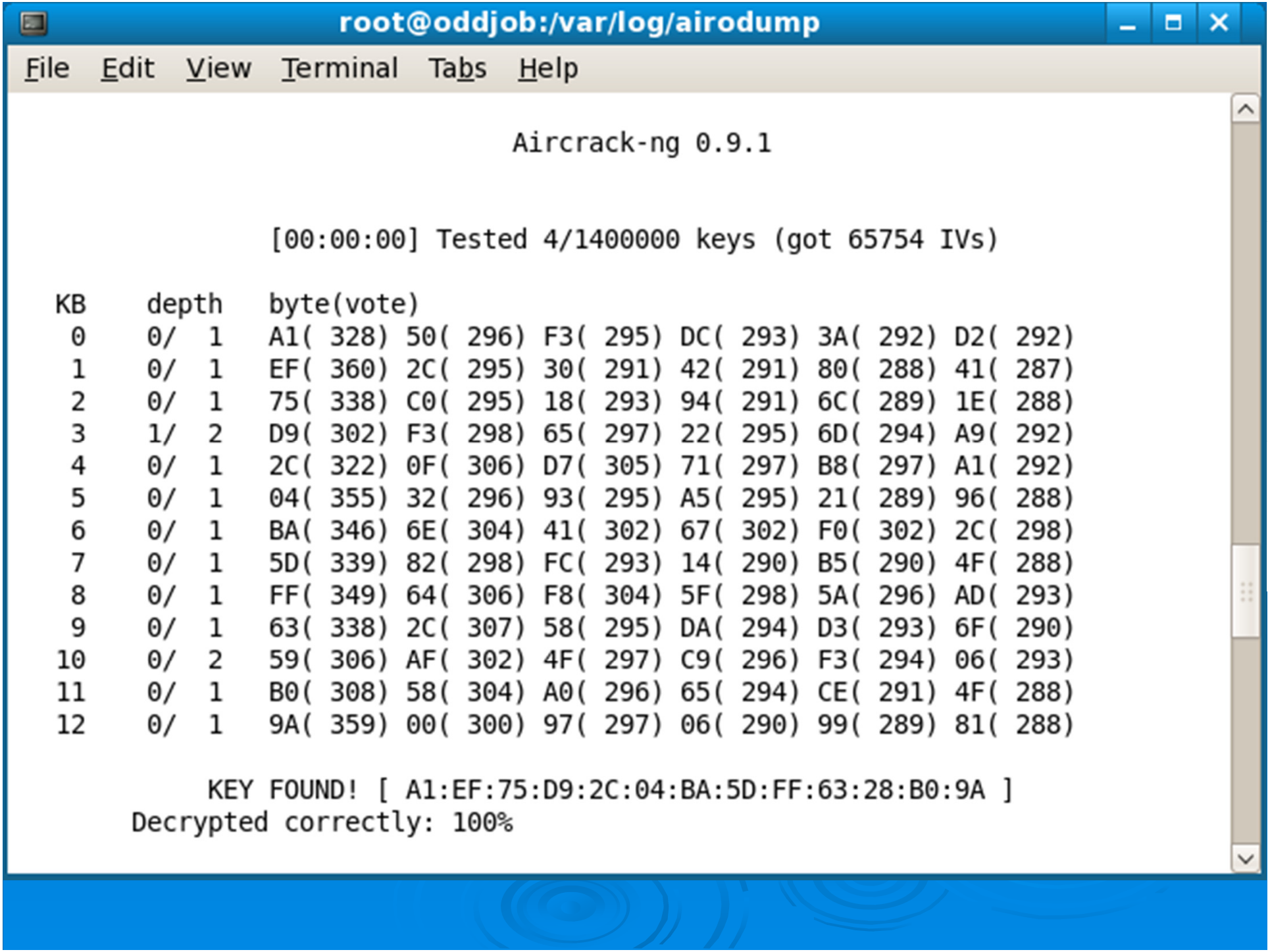
```
* Got  163677! unique IVs | fudge factor = 2
* Elapsed time [09:21:14] | tried 1022310 keys at 1821 k/m

KB    depth   votes
 0    0/ 23   27(  35) 2A(  35) D2(  35) D9(  35) 46(  25) 00(  20)
 1    0/ 84   F3( 129) 0C( 127) FA( 126) E9( 125) F1( 125) 21( 121)
 2    3/ 10   F8(  50) 29(  48) 08(  43) 31(  43) 49(  40) FA(  40)
 3    1/  4   0B(  65) F4(  65) F9(  60) DA(  54) 34(  48) 04(  45)
 4    2/  5   EC(  65) E3(  60) E4(  60) D1(  55) 23(  48) C6(  48)
 5    2/  3   F9( 125) 30(  96) D0(  63) EF(  60) D4(  52) F0(  51)
 6    2/  7   F8( 148) 08( 145) 2F( 103) EC(  90) F0(  90) ED(  85)
 7    4/  5   F0(  75) CB(  63) EE(  60) EF(  60) D0(  49) CD(  48)
 8    2/  4   34( 128) 0D( 125) 0B(  95) EE(  65) D5(  64) CF(  63)
 9    2/  3   F5( 115) B5(  70) 8D(  63) 90(  63) 93(  63) D1(  50)
10    0/  3   A2( 240) CD( 190) C1( 145) AF( 105) B8( 105) AA(  88)
11    0/  3   F3( 235) 1E( 138) 09( 128) 03(  94) 1C(  90) DE(  85)
```

PTW WEP Attacks

- Erik Tews, Ralf-Philipp Weinmann, and Andrei Pyshkin “Breaking 104 bit WEP in less than 60 seconds”
- Includes capture time! (if next to the antenna)
- Needs whole arp reply packets
- aircrack-ng (madwifi-ng) -> aircrack-ptw
- Now aircrack-ng -z


root@oddjob:/var/log/airodump
File Edit View Terminal Tabs Help
Aircrack-ng 0.9.1
[00:03:16] Tested 776160/1400000 keys (got 30600 IVs)
KB depth byte(vote)
0 0/ 7 A1(144) 1B(139) 8C(138) 36(137) 59(137) 50(136)
1 0/ 1 EF(166) 72(142) 21(141) 7E(141) E5(139) 8B(138)
2 0/ 7 75(150) 48(143) 62(143) 14(142) 83(140) 84(140)
3 0/ 1 D9(152) D5(141) D4(138) 65(137) B6(136) 4C(135)
4 4/ 11 2C(138) 29(136) E2(136) 67(135) 76(135) DA(135)
5 0/ 1 04(166) FA(154) 9C(148) 80(147) 9E(142) 51(138)
6 0/ 1 BA(148) 13(137) 44(135) 90(134) 99(134) EA(133)
7 0/ 4 5D(146) B6(143) 73(136) 77(136) 83(135) 90(135)
8 4/ 6 CB(137) 24(136) BC(136) 94(133) A8(133) E4(133)
9 0/ 2 63(150) F2(141) D2(140) 8F(138) 15(137) 7F(136)
10 3/ 10 28(139) CB(138) 8C(137) AC(137) AD(136) 40(135)
11 0/ 1 B0(151) 9D(136) 70(135) 76(135) EB(135) 5E(134)
12 1/ 3 9A(149) 74(142) 6B(139) CC(137) B7(136) DE(136)
KEY FOUND! [A1:EF:75:D9:2C:04:BA:5D:FF:63:28:B0:9A]
Decrypted correctly: 100%


root@oddjob:/var/log/airodump
File Edit View Terminal Tabs Help
Aircrack-ng 0.9.1
[00:00:00] Tested 4/1400000 keys (got 65754 IVs)
KB depth byte(vote)
0 0/ 1 A1(328) 50(296) F3(295) DC(293) 3A(292) D2(292)
1 0/ 1 EF(360) 2C(295) 30(291) 42(291) 80(288) 41(287)
2 0/ 1 75(338) C0(295) 18(293) 94(291) 6C(289) 1E(288)
3 1/ 2 D9(302) F3(298) 65(297) 22(295) 6D(294) A9(292)
4 0/ 1 2C(322) 0F(306) D7(305) 71(297) B8(297) A1(292)
5 0/ 1 04(355) 32(296) 93(295) A5(295) 21(289) 96(288)
6 0/ 1 BA(346) 6E(304) 41(302) 67(302) F0(302) 2C(298)
7 0/ 1 5D(339) 82(298) FC(293) 14(290) B5(290) 4F(288)
8 0/ 1 FF(349) 64(306) F8(304) 5F(298) 5A(296) AD(293)
9 0/ 1 63(338) 2C(307) 58(295) DA(294) D3(293) 6F(290)
10 0/ 2 59(306) AF(302) 4F(297) C9(296) F3(294) 06(293)
11 0/ 1 B0(308) 58(304) A0(296) 65(294) CE(291) 4F(288)
12 0/ 1 9A(359) 00(300) 97(297) 06(290) 99(289) 81(288)
KEY FOUND! [A1:EF:75:D9:2C:04:BA:5D:FF:63:28:B0:9A]
Decrypted correctly: 100%

IEEE 802.11 WLAN Standards (cont'd)

- IEEE 802.11i – MAC Security Enhancements
- IEEE 802.11j – 4.9 GHz - 5 GHz Operation in Japan
- IEEE Std 802.11-2007: A new release (ma) of the standard that includes amendments a, b, d, e, g, h, i & j. (July 2007)
- IEEE 802.11k – Radio Resource Measurement (2008)
- (There is no confusing 'l' or '0')
- IEEE 802.11m,ma,mb – Maintenance of IEEE Std 802.11
- IEEE 802.11n: Higher throughput using MIMO (multiple input, multiple output antennas) (Sept 2009)
- IEEE 802.11p: WAVE:Wless Access for Veh Env (Jul 2010)
- IEEE 802.11r: Fast BSS transition (for VoFi) (2008)
- IEEE 802.11s: Mesh Networking, Extended Service Set (~)

IEEE 802.11n MIMO

- “**t x r : c**”
- Number of transmit antennae
- Number of receive antennae
- Number of spatial channels

- Current gear is 2x2:2, 2x3:2, 3x3:2 – all the same
- Range from ~100Mbps to max300Mbps depending on band size and Guard Interval
- Full certification is 3x3:3 up to 450 Mbps
- Actual standard goes to 4x4:4 up to 600 Mbps

IEEE 802.11i – MAC Security

- Took a long time to be ratified, industry started implementing parts of the draft IEEE 802.11i/D3
- Resolves confidentiality and integrity issues, including authentication, of all **data** frames – management frames remain unprotected
- Uses IEEE 802.1X for authentication, specifies key management algorithms and two data encapsulation mechanisms…

CCMP and TKIP

- Why our industry has a bad name…
- Acronyms of acronyms! – CCMP means:
- The Advanced Encryption Standard algorithm in counter mode with cipher block chaining with message authentication code protocol
- [AES] in CTR mode, with CBC, with MAC (CCM) Protocol (CCMP)
- Temporal Key Integrity Protocol (TKIP)

What They Do

- Temporal Key Integrity Protocol (TKIP)
  - Legacy hardware for WEP
  - MIC called Michael
  - Per-frame keying
- AES in Counter-Mode/CBC-MAC Protocol (CCMP)
  - New hardware
  - Stronger than TKIP
  - AES in counter mode with 128-bit blocks and 128-bit key
  - Authentication & integrity via Cipher Block Chaining Message Authentication Code

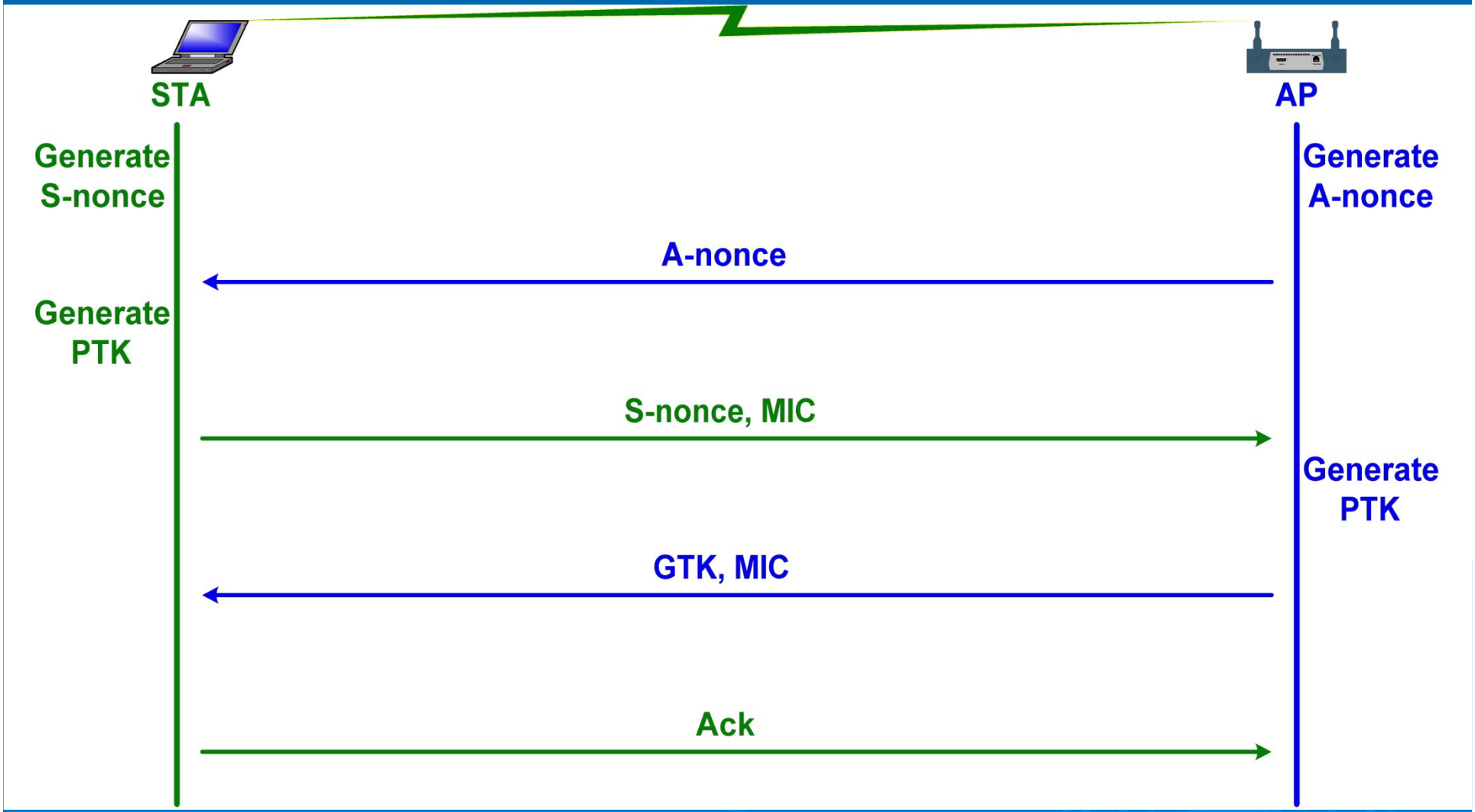
IEEE 802.1X use in IEEE 802.11i

- Supplicant, Authenticator, Authentication Server
- IEEE 802.1X is used between client NIC and AP
  - The protocol between the AP and AS is typically the Remote Authentication Dial-In User Service (RADIUS)
- 2-way Authentication
- Protocol negotiation and key exchanges
  - Authentication and negotiation parameters verified again as part of key exchanges

Robust Security Network (RSN)

- Allows only the creation of robust security network associations (**RSNA**s)…
- …being associations “if the procedure to establish authentication or association between them includes **the 4-Way Handshake**”

The 4-Way Handshake



The 4-way handshake in more detail

- Message 1: Authenticator nonce, seq, PMK-id
  - PTK = Hash(PMK, ANonce, SNonce,
  - supplicant's MAC addr, AP's MAC addr)
- Message 2: Supplicant nonce, RSN IE, seq, MIC
  - PTK = Hash(PMK, ANonce, SNonce,
  - supplicant's MAC addr, AP's MAC addr)
- Message 3: Anonce, RSN IE, GTK, seq+1, MIC
- Message 4: seq+1, MIC

RSNA Requirements

- Protocol Implementation Conformance Statement (PICS)
- RSNA **optional**, but if implemented:
  - RSN Information Element (IE) is mandatory
  - Implementation of CCMP is mandatory
  - A RSN **only allows** RSNAs
  - RSNAs can use either TKIP or CCMP

RSN and TSN

- An AP in a RSN must not associate with pre-RSNA STAs (no RSN IE in the Association Request)
- AP must include the RSN IE in Beacon frames, showing group cipher CCMP or TKIP, but not WEP
- A network that allows creation of pre-RSNAs as well as RSNAs is a **transition security network (TSN)**
- Identified by RSN IE showing the group cipher WEP

Cipher Suite Combinations in RSN IE

Pairwise	**Groupwise**	
CCMP	CCMP	(RSN)
CCMP	TKIP	(RSN)
CCMP, TKIP	TKIP	(RSN)
TKIP	TKIP	(RSN)
CCMP	WEP-40 or WEP-104	(TSN)
CCMP, TKIP	WEP-40 or WEP-104	(TSN)
TKIP	WEP-40 or WEP-104	(TSN)
UseGroup	WEP-40 or WEP-104	(TSN)

Wi-Fi Protected Access (WPA)

- Snapshot of the IEEE 802.11i/D3 draft
- Addressed infrastructure mode WEP vulnerabilities
- “WPA is not available in ad hoc mode”
- Uses the Temporal Key Integrity Protocol (TKIP)
- WPA Personal Mode offer only pre-shared key
- WPA Enterprise Mode offer both PSK and IEEE 802.1X/EAP authentication

Wi-Fi Protected Access (WPA)

- IEEE 802.11i Transition Security Network (TSN)
  - Snapshot of the IEEE 802.11i drafts
  - Addressed WEP vulnerabilities in infrastructure mode
  - “WPA is not available in ad hoc mode” (Wi-Fi Alliance)
  - Uses the Temporal Key Integrity Protocol (TKIP)
  - “Devices can not service a mixture of WEP and WPA”
- WPA Personal Mode offer only pre-shared key
- WPA Enterprise Mode offer both PSK and IEEE 802.1X/EAP authentication

WPA Status

- Uses TKIP for both pairwise and groupwise – RSN?
- NO – It forms a TSN
- Does not (have to) implement the mandatory CCMP
- Does not use the RSN IE (WPA IE is different)
- Does not use RSNAs (WPA 4-way handshake is different to [IEEE 802.11i] "**the** 4-way handshake")
- Although not supposed to service a mixture of WEP and WPA, **many vendors do**, as an extra

WPA “4-way” handshake

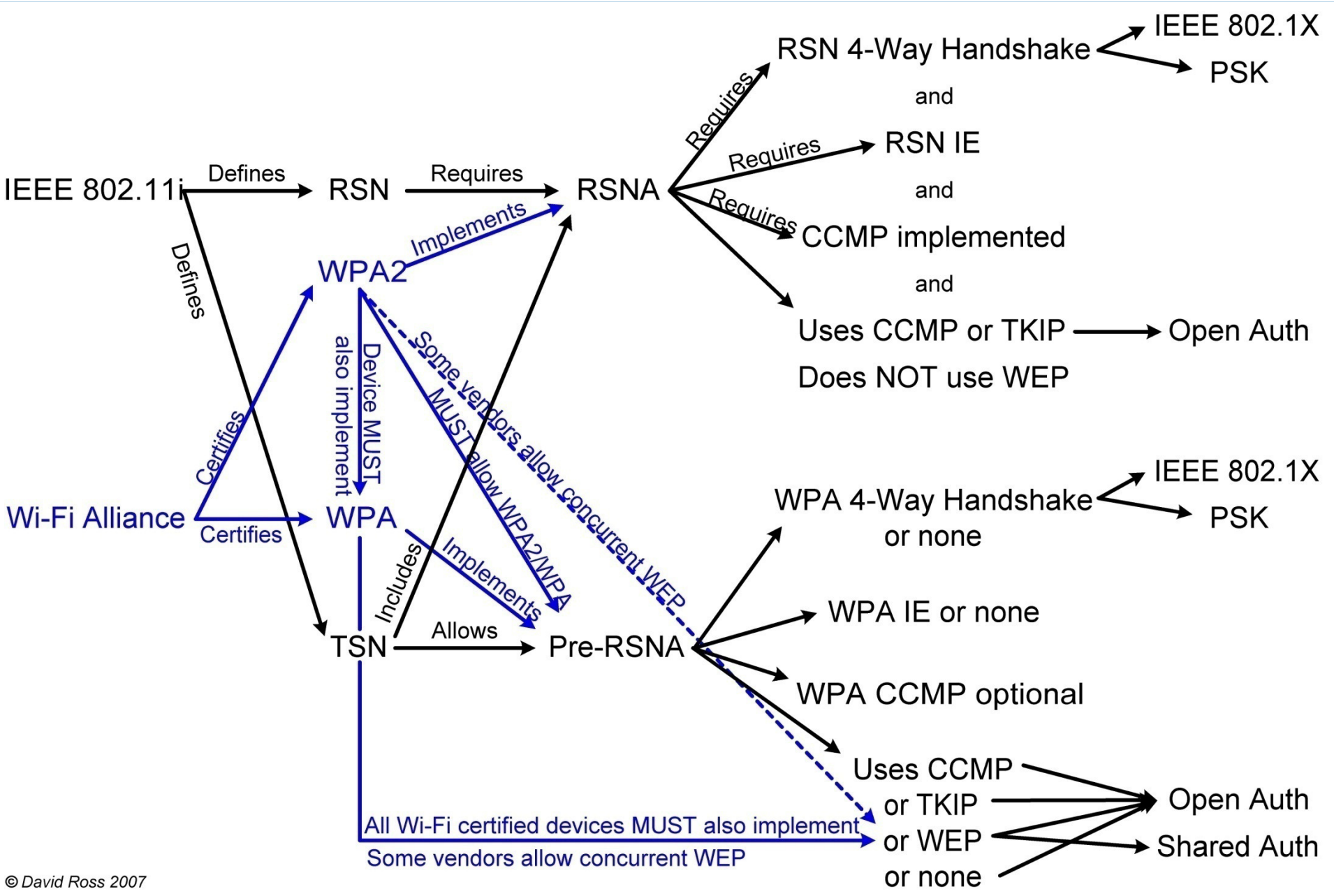
- WPA cannot establish with just a 4-way handshake
- Must also perform an immediate GTK handshake
- Message 1: Authenticator nonce, seq, PMK-id
  - PTK = Hash(PMK, ANonce, SNonce,
  - supplicant’s MAC addr, AP’s MAC addr)
- Message 2: Supplicant nonce, IE, seq, MIC
  - PTK = Hash(PMK, ANonce, SNonce,
  - supplicant’s MAC addr, AP’s MAC addr)
- Message 3: Authenticator nonce, IE, seq+1, MIC
- Message 4: seq+1, MIC

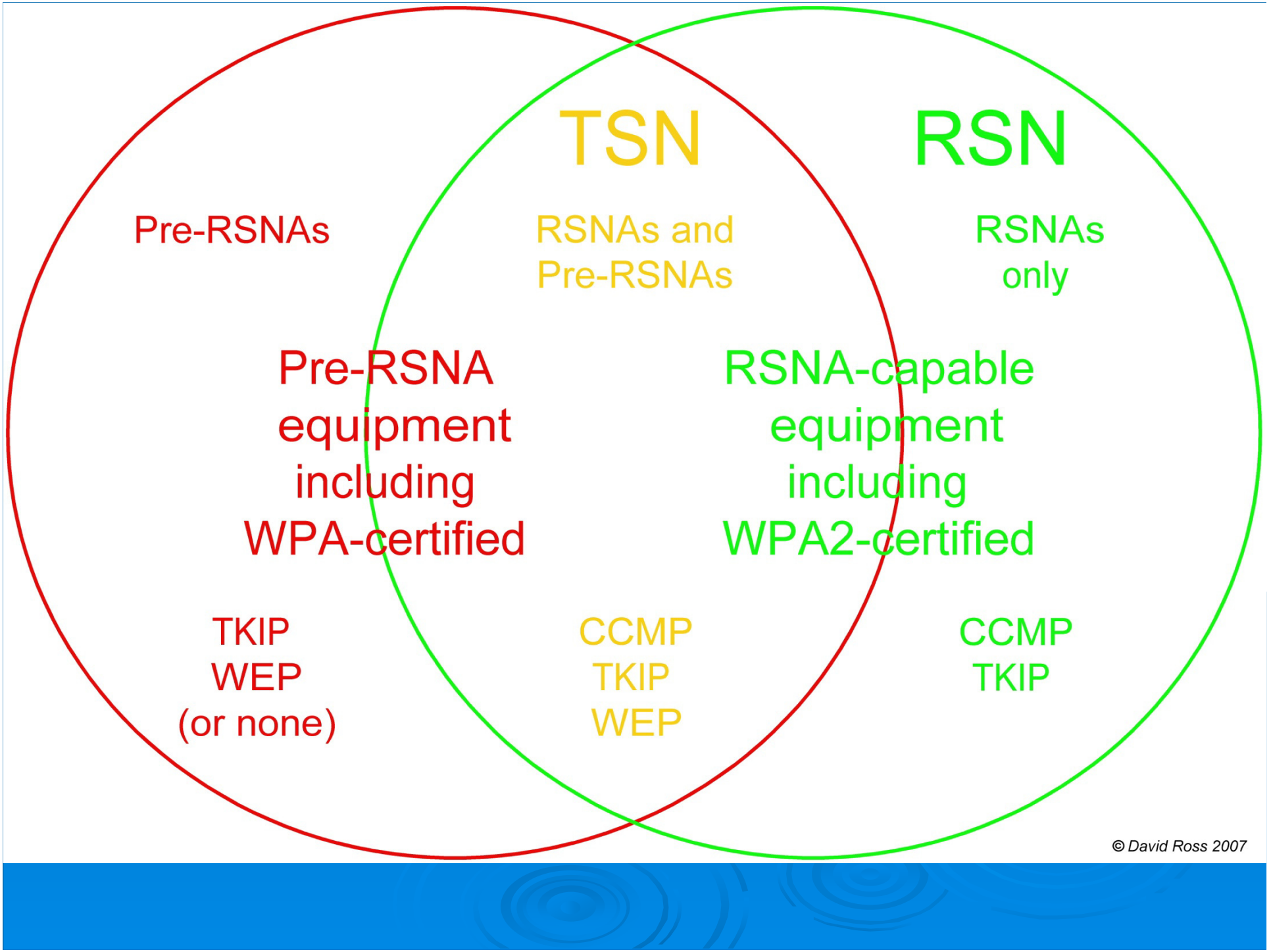
WPA2

- Implements IEEE 802.11i but differs to allow for interoperability with WPA
- Available in both infrastructure mode and ad hoc
- WPA2 provides both TKIP and AES-CCMP
- An Access Point and client card running only CCMP in WPA2 will be running an IEEE 802.11i Robust Security Network (RSN)
- An AP that allows WPA clients will be running a Transition Security Network (TSN)

WPA vs WPA2

- WPA only certified for Infrastructure, not Ad Hoc
- In WPA, only TKIP is 'certified‘, but may do AES
- WPA2 must provide both TKIP and AES-CCMP
- WPA doesn’t do PMK caching or pre-authentication
- WPA 4-way handshake is different
- WPA IE and (WPA2) RSN IE are different!


IEEE 802.11i
Defines
RSN
Requires
RSNA
RSN 4-Way Handshake
IEEE 802.1X
PSK
and
Requires
RSN IE
and
Requires
CCMP implemented
and
Uses CCMP or TKIP
Open Auth
Does NOT use WEP
Defines
WPA2
Implements
Certifies
Device MUST also implement
Some vendors allow concurrent WEP
MUST allow WPA2/WPA
Wi-Fi Alliance
Certifies
WPA
WPA 4-Way Handshake
or none
IEEE 802.1X
PSK
Includes
Implements
WPA IE or none
TSN
Allows
Pre-RSNA
WPA CCMP optional
Uses CCMP
or TKIP
or WEP
or none
Open Auth
Shared Auth
All Wi-Fi certified devices MUST also implement
Some vendors allow concurrent WEP
© David Ross 2007


TSN
RSN
Pre-RSNAs
RSNAs and Pre-RSNAs
RSNAs only
Pre-RSNA equipment including WPA-certified
RSNA-capable equipment including WPA2-certified
TKIP
WEP
(or none)
CCMP
TKIP
WEP
CCMP
TKIP
© David Ross 2007

When ‘WPA2’ implements a TSN

- WPA2 “TKIP+CCMP” often WPA-compatibility
- Wi-Fi certifies, **in default configuration**, WPA2 mode doesn’t allow simultaneous WEP
- Each Wi-Fi certified device must support WEP
- Many vendors permit a mixture of WPA2/WPA or WPA/WEP or even all three at once

WPA2/WPA TSN Risk

- TSN is weaker than RSN
- WPA-PSK (or WPA2-PSK) PMK is a hash of the PSK passphrase – weak passphrases considerably decrease the key strength
- PSK dictionary passwords destroy all security

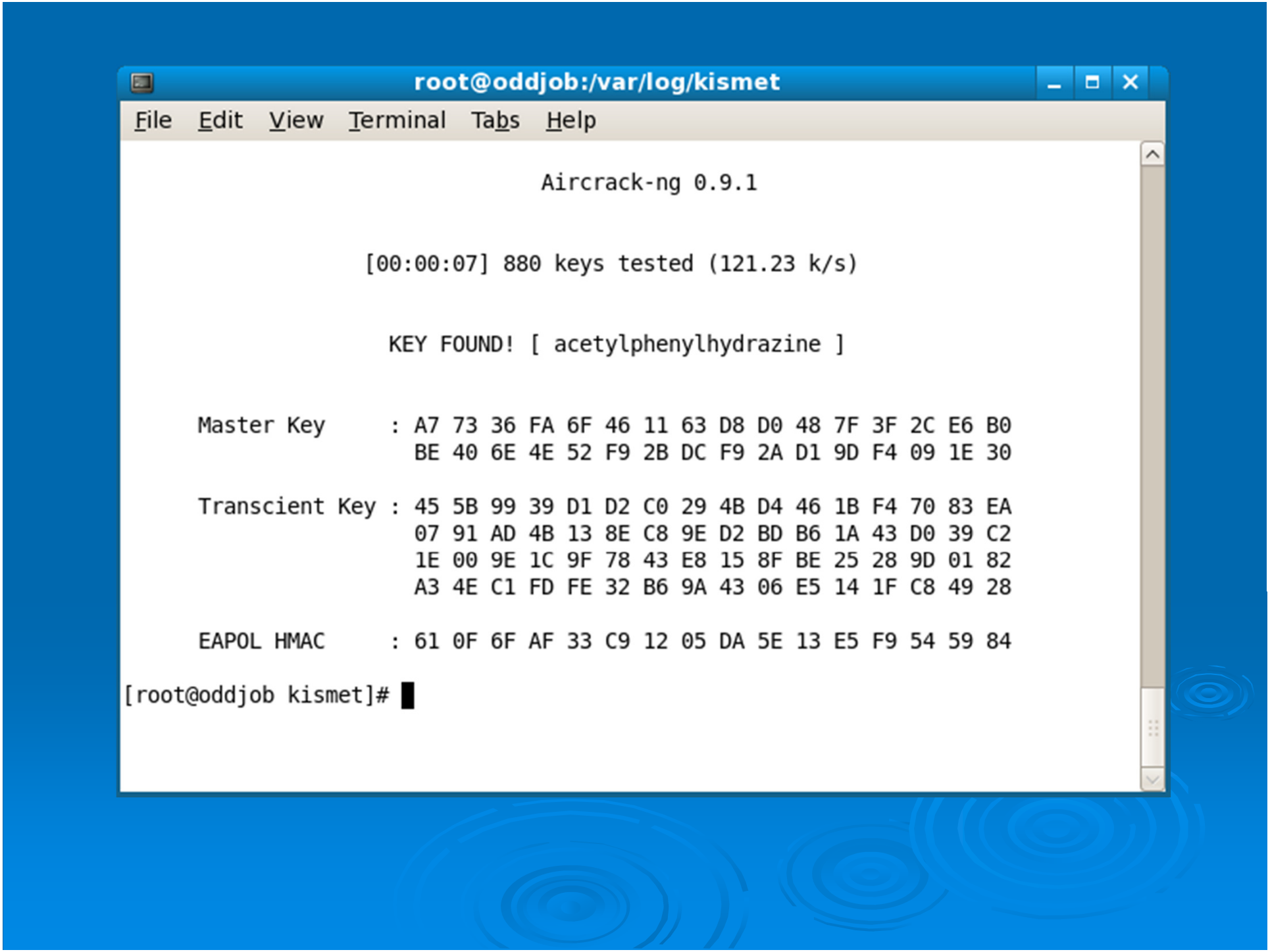
WPA2-PSK

- 64 hex characters = 256 bits
- 8-63 printable ASCII characters = 64-504 bits
- printable ASCII characters hashed to 256 bits

- How much entropy?
  - 64 random hex characters = ?? bits
  - 8-63 printable ASCII characters = ?? bits

WPA2-PSK

- How many to use minimum?
  - 12 characters?
  - 15 characters?
  - Many say at least 20 characters
- acetylaminofluorine (19)
- acetylphenylhydrazine (20)


root@oddjob:/var/log/kismet
File Edit View Terminal Tabs Help
Aircrack-ng 0.9.1
[00:00:07] 880 keys tested (121.23 k/s)
KEY FOUND! [acetylphenylhydrazine]
Master Key : A7 73 36 FA 6F 46 11 63 D8 D0 48 7F 3F 2C E6 B0
BE 40 6E 4E 52 F9 2B DC F9 2A D1 9D F4 09 1E 30
Transcient Key : 45 5B 99 39 D1 D2 C0 29 4B D4 46 1B F4 70 83 EA
07 91 AD 4B 13 8E C8 9E D2 BD B6 1A 43 D0 39 C2
1E 00 9E 1C 9F 78 43 E8 15 8F BE 25 28 9D 01 82
A3 4E C1 FD FE 32 B6 9A 43 06 E5 14 1F C8 49 28
EAPOL HMAC : 61 0F 6F AF 33 C9 12 05 DA 5E 13 E5 F9 54 59 84
[root@oddjob kismet]#

WPA2/WEP TSN Risk

- Network strength reduced to WEP
- Can passively capture packets for attack in hours
- Can actively capture packets for attack in minutes
- Can execute FMS attack in hours to days
- Can actively capture ARP packets in minutes
- Can execute PTW attack in seconds
- Mixing WEP destroys all WPA/WPA2 security

Transition Risk

- Running mixed modes
- Retire the last of the legacy equipment
- All devices now using CCMP
- Do we now have a RSN?
- NO – must reconfigure to refuse pre-RSNAs
- Old PC in storeroom powers up w/ WEP
- Attacker captures ARPs and recovers key

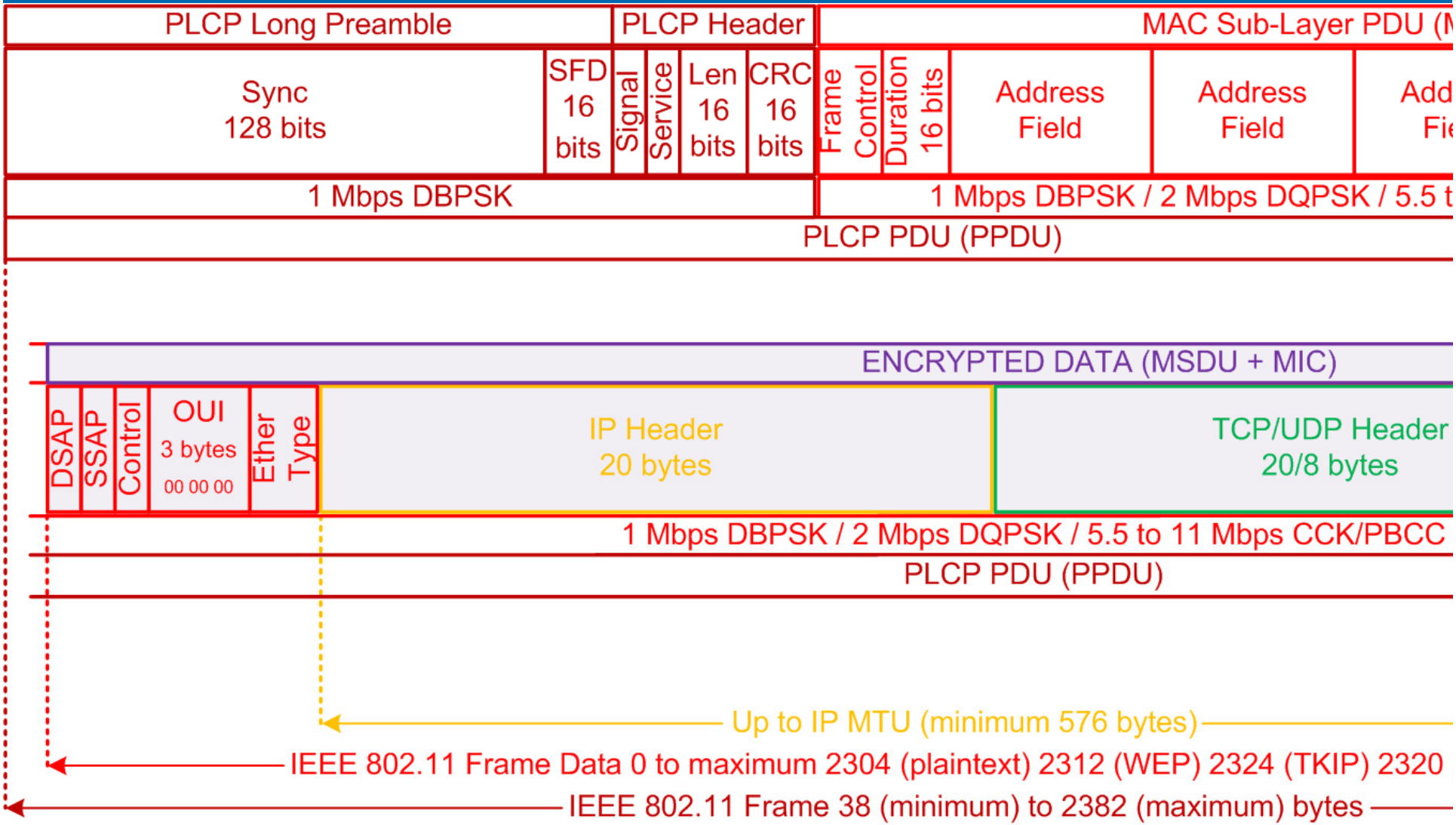
KRACK

- Wireless Security Vulnerability - KRACK
- Affects WPA and WPA2 implemnataions
  - Both PSK and IEEE 802.1X.
- 10 CVE's (Common Vulnerabilities and Exposures) have been released:
  - 9 are client based and
  - 1 is infrastructure based.
- All 10 CVE's are implementation issues which means patches can fix the vulnerability

KRACK

- The 4-way handshake is prone to replay attacks (man-in-the-middle / MITM).
- User de-auth'ed from the AP causing them to potentially re-connect to the MITM AP.
- Replay of message 3 will set the same key back in place BUT RE-INITIALISE ALL COUNTERS – SO NONCES CAN BE RE-USED
- Known plaintext can be used to determine keystream – and thus decrypt ciphertext

Frame Formats



Authentication Frame Format

Deauthentication/Disassociation

Type: 0 (Mgt) – Subtype: 12 (Deauthentication)+00						
0x00b0	Duratn	Destination Address 6 bytes	Source Address 6 bytes	BSSID (AP / IBSS) 6 bytes	Sequence Control	Reason

Type: 0 (Mgt) – Subtype: 10 (Disassociation)						
0x0010	Duratn	Destination Address 6 bytes	Source (AP addr) 6 bytes	BSSID (AP addr) 6 bytes	Sequence Control	Reason

Management Frames

- Working groups considerably extending the functionality of management frames to include sensitive information, such as:
  - radio resource data
  - location-based identifiers
  - fast-roaming information, and
  - wireless network management
- Security in wireless networks needs to be extended to management frames as well as data frames.

IEEE 802.11w

- Provides (some) Protected Management Frames
- provides mechanisms that enable
  - data integrity
  - data origin authenticity
  - replay protection
  - data confidentiality
- (for selected management frames)
- Provides protection against:
  - Injection attacks
  - Disassociation attacks
  - Fake APs
- Ratified September 2009 but nobody advertising!
- Except CISCO who were a major player in the standard

Any questions?