



Last updated 9/16/2016

Rich's lesson module checklist

- Slides and lab posted
- WB converted from PowerPoint
- Print out agenda slide and annotate page numbers

- Flash cards
- Properties
- Page numbers
- 1st minute quiz
- Web Calendar summary
- Web book pages
- Commands

- Lab 2 posted and tested
- Sample Lab 2 posted

- Rosters printed
- Add codes printed

- Backup slides, whiteboard slides, CCC info, handouts on flash drive
- Spare 9v battery for mic
- Key card for classroom door



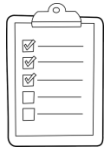
Student checklist for attending class

The screenshot shows a web browser window with the URL simms-teach.com/cis90calendar.php. The page title is "Rich's Cabrillo College CIS Classes CIS 90 Calendar". There are navigation buttons for "Home", "Calendar", "CIS 76", "CIS 77", "CIS 78", "CIS 79", "CIS 80", "CIS 81", "CIS 82", "CIS 83", "CIS 84", "CIS 85", "CIS 86", "CIS 87", "CIS 88", "CIS 89", "CIS 90", "CIS 91", "CIS 92", "CIS 93", "CIS 94", "CIS 95", "CIS 96", "CIS 97", "CIS 98", "CIS 99", "CIS 100". The "CIS 76" button is highlighted. Below the navigation buttons, there is a "CIS 90 (Fall 2014) Calendar" section with tabs for "Course Home", "Syllabus", and "Calendar". The "Calendar" tab is selected. A table shows the lesson details for CIS 76:

Lesson	Date	Topics	Link
CIS 76	9/2	<p>Class and Linux Operations</p> <ul style="list-style-type: none"> Understand how the course will work High-level overview of computers, operating systems and virtual machines Overview of UNIX/Linux market and architecture Using SSH for remote network logs Using terminals and the command line <p>Materials</p> <p>Presentation slides (download)</p> <p>Supplemental</p> <ul style="list-style-type: none"> PowerPoint: Logging into Opus (download) <p>Assignments</p> <ul style="list-style-type: none"> Student Survey Lab 1 <p>CIS 76 Files</p> <p>Enter virtual classroom</p>	

1. Browse to:
<http://simms-teach.com>
2. Click the **CIS 76** link.
3. Click the **Calendar** link.
4. Locate today's lesson.
5. Find the **Presentation slides** for the lesson and **download** for easier viewing.
6. Click the **Enter virtual classroom** link to join CCC Confer.
7. Log into Opus with Putty or ssh command.

Note: Blackboard Collaborate Launcher only needs to be installed once. It has already been downloaded and installed on the classroom PC's.



Student checklist for suggested screen layout

Google

CCC Confer

Downloaded PDF of Lesson Slides

The screenshot shows a virtual classroom interface. On the left is a sidebar with navigation options like 'Login', 'Flashcards', 'Admin', and 'CIS 90 (Spring)'. The main area displays a 'Class Activity - Where are you now?' slide with a Google map of San Jose, CA. A 'CCC Confer' window is open, showing a video feed of 'Rich Simms' and a list of participants. A 'cis90lesson01.pdf' window is open in the background, showing a slide titled 'The CIS 90 System Playground'. A terminal window in the bottom right shows a password prompt and a welcome message: 'Welcome to Opus serving Cabrillo College'. A checklist overlay is present, with blue arrows pointing to various elements: 'Google' points to the map; 'CCC Confer' points to the confer window; 'Downloaded PDF of Lesson Slides' points to the PDF window; 'CIS 76 website Calendar page' points to the sidebar; and 'One or more login sessions to Opus' points to the terminal window.

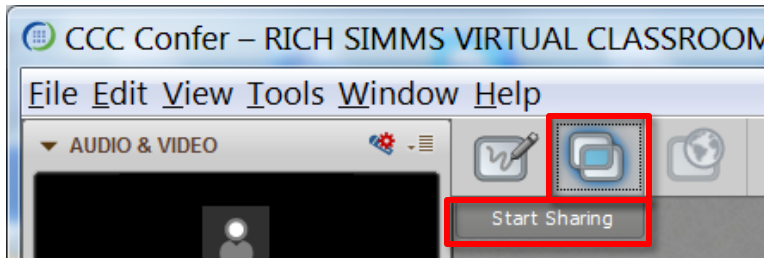
CIS 76 website Calendar page

One or more login sessions to Opus

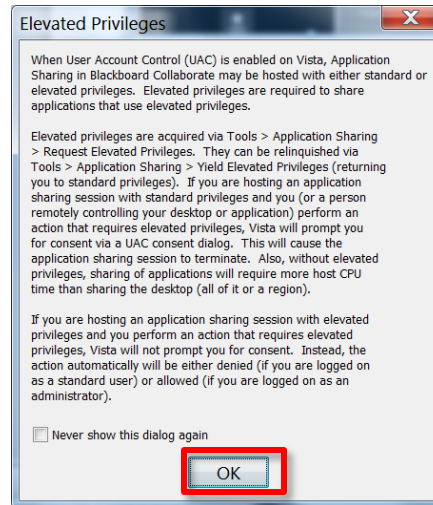


Student checklist for sharing desktop with classmates

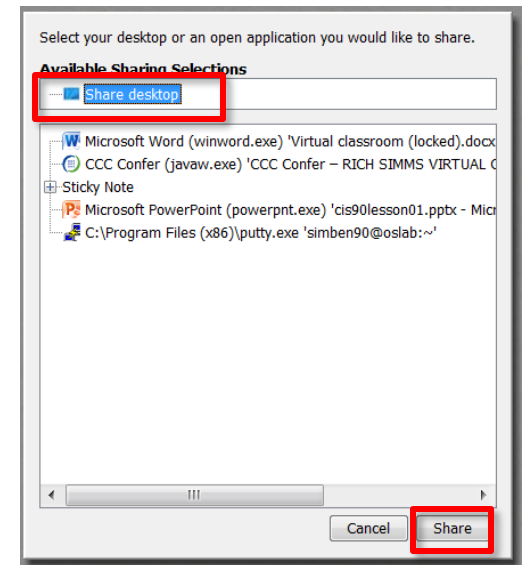
1) Instructor gives you sharing privileges.



2) Click overlapping rectangles icon. If white "Start Sharing" text is present then click it as well.



3) Click OK button.



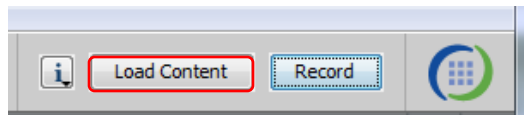
4) Select "Share desktop" and click Share button.



Rich's CCC Confer checklist - setup

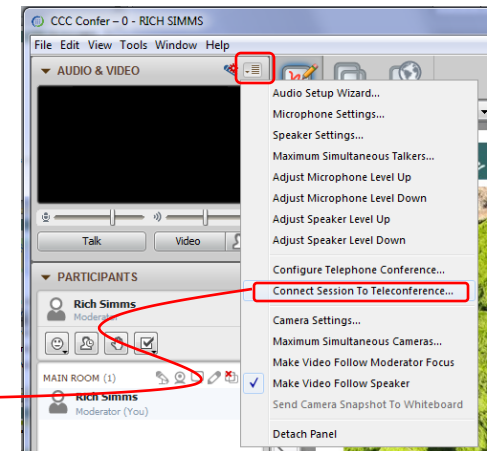
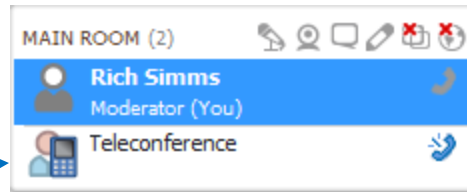


[] Preload White Board



[] Connect session to Teleconference

Session now connected to teleconference



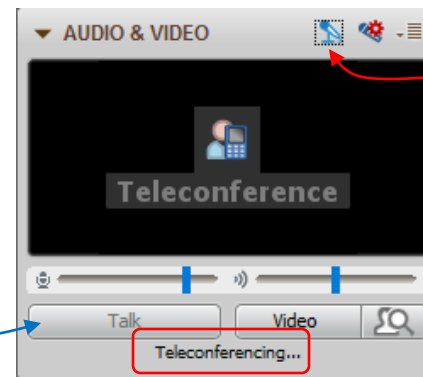
[] Is recording on?



Red dot means recording

[] Use teleconferencing, not mic

Should be grayed out



Should change from phone handset icon to little Microphone icon and the Teleconferencing... message displayed



Rich's CCC Confer checklist - screen layout



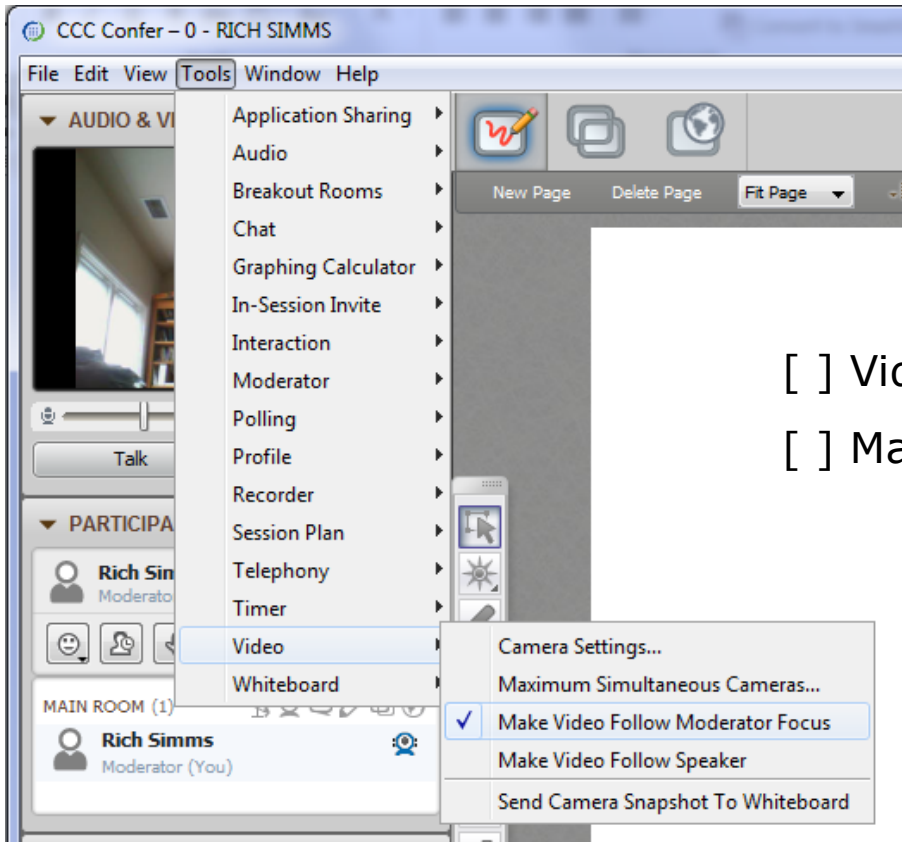
The screenshot displays a Windows desktop environment with several applications open. On the left is the CCC Confer window, showing a video feed of Rich Simms and a list of participants. In the center is a Chrome browser window displaying a PDF document titled 'cis90-TEST-1-Fall-12.pdf'. Overlaid on the Chrome window is a Putty terminal window showing a login session for 'simben90@oslab'. On the right is the vSphere Client window, showing the vCenter interface. Three red callout boxes with white text are overlaid on the image: 'foxit for slides' points to the PDF document, 'chrome' points to the browser window, and 'vSphere Client' points to the vSphere Client window. The desktop taskbar at the bottom shows icons for various applications, including Internet Explorer, Firefox, and Microsoft Word.

[] layout and share apps





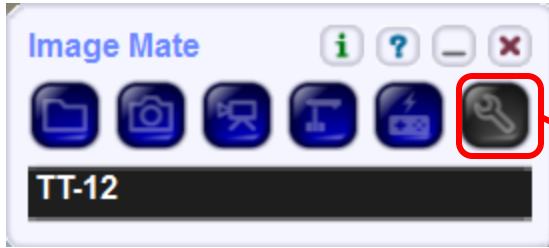
Rich's CCC Confer checklist - webcam setup



- [] Video (webcam)
- [] Make Video Follow Moderator Focus



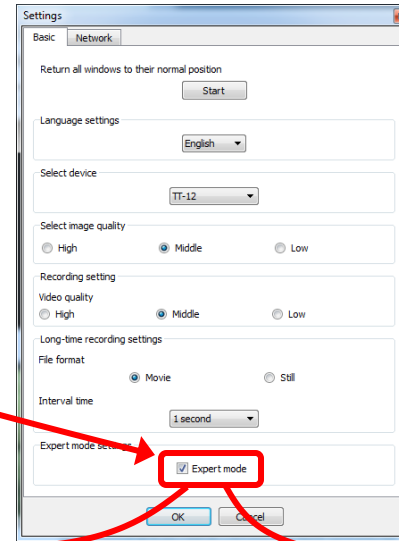
Rich's CCC Confer checklist - Elmo



Elmo rotated down to view side table



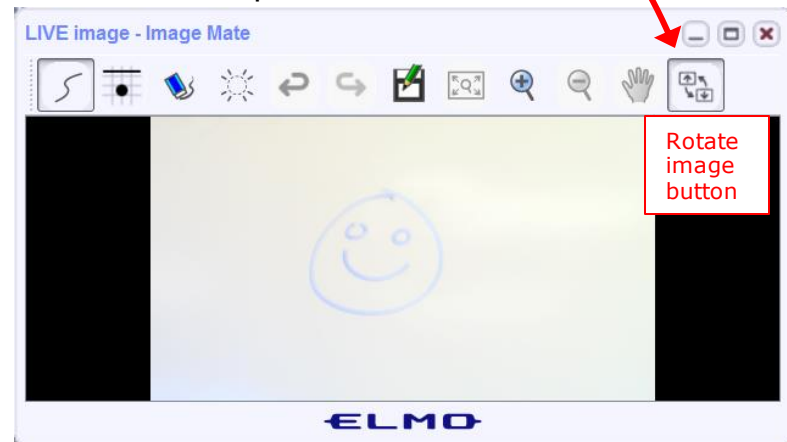
Run and share the Image Mate program just as you would any other app with CCC Confer



The "rotate image" button is necessary if you use both the side table and the white board.

Quite interesting that they consider you to be an "expert" in order to use this button!

Elmo rotated up to view white board





Rich's CCC Confer checklist - universal fixes

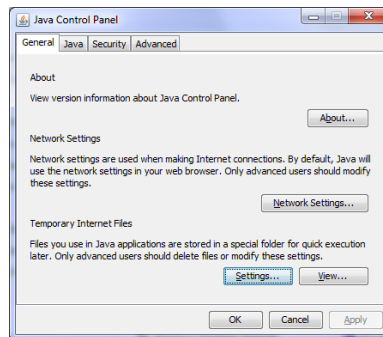
Universal Fix for CCC Confer:

- 1) Shrink (500 MB) and delete Java cache
- 2) Uninstall and reinstall latest Java runtime
- 3) <http://www.cccconfer.org/support/technicalSupport.aspx>

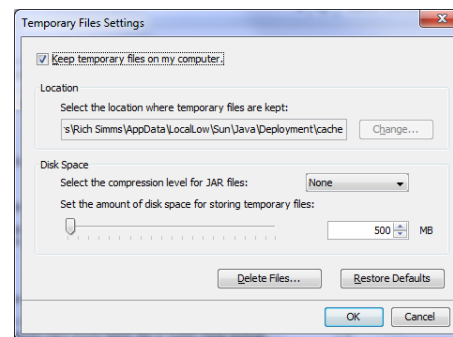
Control Panel (small icons)



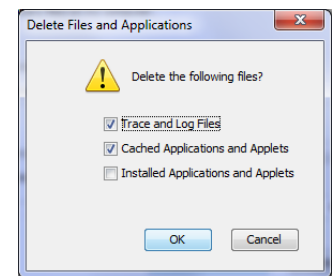
General Tab > Settings...



500MB cache size



Delete these



Google Java download



Start

Sound Check

*Students that dial-in should mute their line using *6 to prevent unintended noises distracting the web conference.*

*Instructor can use *96 to mute all student lines.*

First Minute Quiz

Please answer these questions **in the order** shown:

Use CCC Confer White Board

email answers to: risimms@cabrillo.edu

(answers must be emailed within the first few minutes of class for credit)

TCP/IP Review

Objectives

- Review the TCP/IP protocol stack
- Review IP addressing

Agenda

- Quiz #1
- Certifications
- Vocabulary
- Conferences
- Newsletters and Blogs
- TCP/IP model
- Network Access layer
- Internet layer
- Transport layer
- Application layer
- Assignment
- Wrap up

Introductions and Credits



Rich Simms

- HP Alumnus.
- Started teaching in 2008 when Jim Griffin went on sabbatical.
- Rich's site: <http://simms-teach.com>

And thanks to:

- Steven Bolt at for his WASTC EH training.
- Kevin Vaccaro for his CSSIA EH training and Netlab+ pods.
- EC-Council for their online self-paced CEH v9 course.
- Sam Bowne for his WASTC seminars, textbook recommendation and fantastic EH website (<https://samsclass.info/>).
- Lisa Bock for her great lynda.com EH course.
- John Govsky for many teaching best practices: e.g. the First Minute quizzes, the online forum, and the point grading system (<http://teacherjohn.com/>).
- Google for everything else!

Credits

Rick Graziani



- Thanks to Rick Graziani for the use of some of his great network slides
- Rick's site:
<http://www.cabrillo.edu/~rgraziani/>



Instructor: **Rich Simms**

Dial-in: **888-886-3951**

Passcode: **136690**



Jordan



Ryan



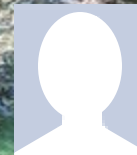
Takashi



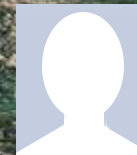
Karl-Heinz



Sean



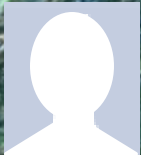
Benji



Joshua



Brian



Tess



Jeremy



David H.



Roberto



Nelli



Mike C.



Deryck



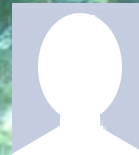
Alex



Michael W.



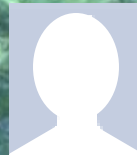
Carter



Thomas



Wes



Jennifer



Marcos



Tim



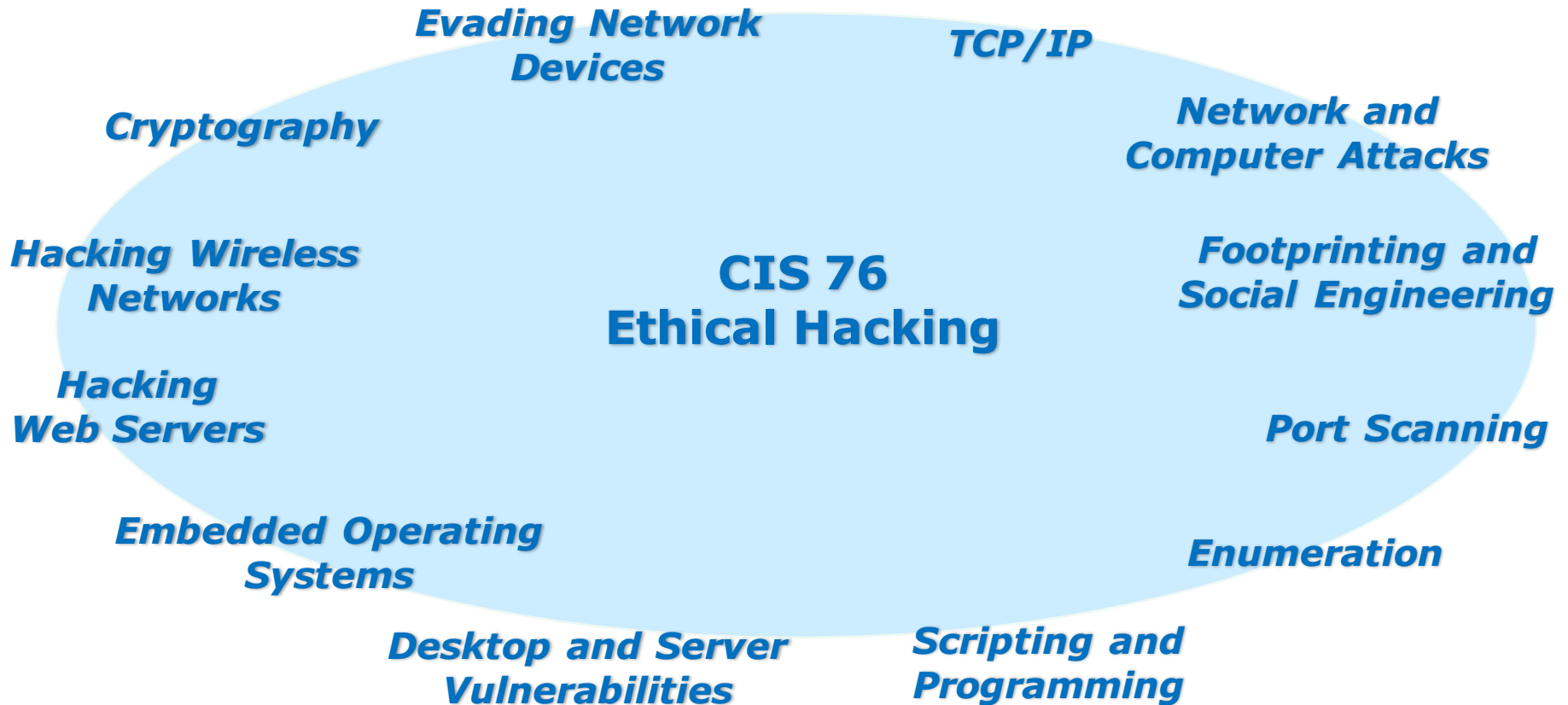
Daniel



Dave R.



Luis



Student Learner Outcomes

1. Defend a computer and a LAN against a variety of different types of security attacks using a number of hands-on techniques.
2. Defend a computer and a LAN against a variety of different types of security attacks using a number of hands-on techniques.

Admonition



Unauthorized hacking is a crime.

The hacking methods and activities learned in this course can result in prison terms, large fines and lawsuits if used in an unethical manner. They may only be used in a lawful manner on equipment you own or where you have explicit permission from the owner.

Students that engage in any unethical, unauthorized or illegal hacking may be dropped from the course and will receive no legal protection or help from the instructor or the college.



Questions

Questions

How this course works?

Past lesson material?

Previous labs?

Chinese
Proverb

他問一個問題，五分鐘是個傻子，他不問一個問題仍然是一個傻瓜永遠。

He who asks a question is a fool for five minutes; he who does not ask a question remains a fool forever.



Certifications

	SB	KV	Simpson Textbook	<u>Concise Cybersecurity</u>
A+ (CompTIA)		1		
Linux Essentials (LPI)		3		
Linux+ (CompTIA)	x			
Network+ (CompTIA)		2	x	
Security+ (CompTIA)	1	4	x	x
CISSP (ISC ²)		6a	x	
CEH (EC-Council)	2	5	x	x
GPEN (SANS/GIAC)	3	6b	x	x
OPST (ISECOM)			x	
OSCP (Offensive Security)	x			x



Vocabulary

Some Terminology

- Hacking
- Cracking
- White hat hacker
- Grey hat hacker
- Black hat hacker
- Nation-state actors
- Cybercriminals
- Adversary
- Hacktivist
- Pen Test
- Security audit
- White box testing
- Grey box testing
- Black box testing
- Red Team
- Blue Team
- Vulnerability
- Exploit
- Threat
- Denial of Service attack
- Brute force attack
- Buffer overflow
- Spoofing
- Zero-day
- Botnet
- Ransomware ([link](#))
- Watering hole attack ([link](#))
- Man in the middle attack
- Fuzzing ([link](#))
- Drive-by-download ([link](#))
- Cross-site scripting ([link](#))
- SQL injection ([link](#))
- Malware
- Virus
- Trojan ([link](#))
- Worm ([link](#))
- Spyware
- Rootkit ([link](#))
- Firewall
- Signatures ([link](#))
- Polymorphism
- Exfiltrate
- Social engineering
- Phishing
- Vishing ([listen](#))
- Spear-phishing

Acronyms

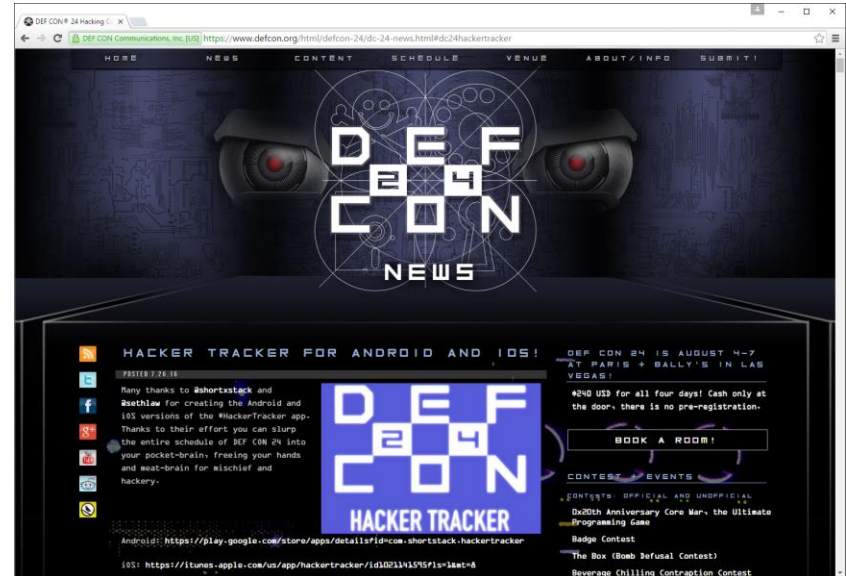
- ❑ CVE (Common Vulnerabilities and Exposures)
- ❑ DoS (Denial of Service attack)
- ❑ DDoS (Distributed Denial of Service attack)
- ❑ XSS (Cross-Site Scripting)
- ❑ IDS (Intrusion Detection System)
- ❑ IPS (Intrusion Prevention System)
- ❑ C&C (Command and Control)
- ❑ AV (Anti-Virus)
- ❑ APT (Advanced Persistent Threat)
- ❑ RAT (Remote Access Trojan)

Slang

- Owned
- Pwned
- Meat chicken ("rouji" in Chinese)
- Doxing
- Script Kiddie
- Packet Monkey



Conferences



Black Hat

DEF CON

And many more: ToorCon, Hackers Halted, RSA, OWASP events, ShmooCon, DerbyCon, Thotcon, USENIX...

Google: youtube defcon

The screenshot shows a Google search interface with the query 'youtube defcon'. The search results are as follows:

- DEFCONConference - YouTube**
<https://www.youtube.com/user/DEFCONConference>
DEF CON Conference. ... DEF CON 23 - Aaron Grattafiori - Linux Containers: Future or Fantasy? ...
DEF CON 23 - Amit Ashbel & Maty Siman - Game of Hacks: Play, Hack & Track - 101 Track - Duration: 31 minutes.
- DEFCON 20: Owned in 60 Seconds: From Network Guest ... - YouTube**
https://www.youtube.com/watch?v=nHU3ujyw_sQ
Aug 21, 2012 - Uploaded by Christiaan008
Speaker: ZACK FASEL Their systems were fully patched, their security team watching, and the amateur ...
- DEF CON Videos - YouTube**
<https://www.youtube.com/user/defconvideos>
Welcome to the only channel purely dedicated to **Defcon**. This channel contains a full list of **Defcon** Conference videos. These videos are not my own and the cr.
- Defcon 21 - Social Engineering: The Gentleman Thief - YouTube**
<https://www.youtube.com/watch?v=1kkOKvPrdZ4>
Nov 16, 2013 - Uploaded by HackersOnBoard
Apollo August 1st-4th, 2013 Rio Hotel & Casino • Las Vegas, Nevada.
- DEF CON 23 - Chris Rock - I Will Kill You - YouTube**
<https://www.youtube.com/watch?v=9FdHq3WfJgs>
Aug 14, 2015 - Uploaded by DEFCONConference
DEFCON 19: Steal Everything, Kill Everyone, Cause Total Financial Ruin! ... [DEFCON 21] Backdoors ...
- DEFCON - The Full Documentary - YouTube**

Looking ahead ...

Sept 10-19 2016, SANS Network Security 2016 Las Vegas

July 22-27 2017, Black Hat USA 2017 Las Vegas

July 27-30 2017, DEF CON 25 Las Vegas

<https://www.concise-courses.com/security/conferences-of-2016/>

<https://www.concise-courses.com/security/conferences-of-2017/>



Newsletters and Blogs

Subscribe or sign up for cyber security newsletters, alerts, blogs and feeds

- US-CERT
- SANS
- Cybrary
- FireEye
- CrowdStrike
- AlienVault
- HackerNews
- Many more ...

Department of Homeland Security - US-CERT

Vulnerability Summary for: x
<https://www.us-cert.gov/ncas/bulletins/SB16-207>
 Official website of the Department of Homeland Security

US-CERT
 UNITED STATES COMPUTER EMERGENCY READINESS TEAM

HOME ABOUT US CAREERS PUBLICATIONS ALERTS AND TIPS RELATED RESOURCES C'VP

Bulletin (SB16-207) More Bulletins
 Vulnerability Summary for the Week of July 18, 2016
 Original release date: July 25, 2016

Print Tweet Send Share

The US-CERT Cyber Security Bulletin provides a summary of new vulnerabilities that have been recorded by the National Institute of Standards and Technology (NIST) National Vulnerability Database (NVD) in the past week. The NVD is sponsored by the Department of Homeland Security (DHS) National Cybersecurity and Communications Integration Center (NCCIC) / United States Computer Emergency Readiness Team (US-CERT). For modified or updated entries, please visit the NVD, which contains historical vulnerability information.

The vulnerabilities are based on the CVE vulnerability naming standard and are organized according to severity, determined by the Common Vulnerability Scoring System (CVSS) standard. The division of high, medium, and low severities correspond to the following scores:

- High** - Vulnerabilities will be labeled High severity if they have a CVSS base score of 7.0 - 10.0
- Medium** - Vulnerabilities will be labeled Medium severity if they have a CVSS base score of 4.0 - 6.9
- Low** - Vulnerabilities will be labeled Low severity if they have a CVSS base score of 0.0 - 3.9

Entries may include additional information provided by organizations and efforts sponsored by US-CERT. This information may include identifying information, values, definitions, and related links. Patch information is provided when available. Please note that some of the information in the bulletins is compiled from external, open source reports and is not a direct result of US-CERT analysis.

High Vulnerabilities				
Primary Vendor - Product	Description	Published	CVSS Score	Source & Patch Info
cisco -- ios_xr	Cisco IOS XR 5.x through 5.2.5 on NCS 6000 devices allows remote attackers to cause a denial of service (timer consumption and Route Processor reload) via crafted SSH traffic, aka Bug ID CSCux76819.	2016-07-15	7.8	CVE-2016-1426 CISCO@P
cisco -- ios_xr	The CLI in Cisco IOS XR 6.x through 6.0.1 allows local users to execute arbitrary OS commands in a privileged context by leveraging unspecified container access.	2016-07-15	7.2	CVE-2016-1456 CISCO@P

SANS Blogs

The screenshot shows the SANS Penetration Testing website. The browser address bar displays the URL: pen-testing.sans.org/blog#_utma=216335632.2090294832.1467909806.1469635543.1469635543.5&_utmb=216335632.5.9.1469638387876&_utmc=216335632&_utmz=-&_utmz=216335632. The website header includes the SANS Penetration Testing logo and navigation links for Resources, Training, Events, Certification, Instructors, and About. A search bar is located in the top right corner.

The main content area features a dark red banner with the text "SANS Penetration Testing". Below this, three blog posts are listed:

- 05 Jul 2016**

Python Cheat Sheet - pyWars (SEC573)

0 comments Posted by [jblanchard](#)
 Filed under [Cheatsheet](#), [Python](#)
 by: Mark Baggett Python skills are incredibly useful for all kinds of information security personnel, from pen testers to cyber defenders to forensics pros. With so many tools written in Python and so many Python libraries to work magic in just a few lines of code, I wrote a course (SANS SEC573) on how to ... [Continue reading Python Cheat Sheet - pyWars \(SEC573\)](#)
- 25 May 2016**

SANS PowerShell Cheat Sheet from SEC560 Course

0 comments Posted by [eskoudis](#)
 Filed under [Cheatsheet](#)
 by Ed Skoudis PowerShell really is amazing, and comes in handy for all kinds of infosec tasks, from defense to analysis to offense. In my SANS Security 560 course, we cover PowerShell as a post-exploitation language, with all kinds of nifty tips and tricks for using it. When I teach the class, though, I notice ... [Continue reading SANS PowerShell Cheat Sheet from SEC560 Course](#)
- 05 Apr 2016**

Scapy Cheat Sheet from SANS SEC560

0 comments Posted by [eskoudis](#)
 Filed under [Scanning](#), [scapy](#)
 One of my favorite tools for fine-grained interactions with target systems during penetration testing is the mightyScapy. While other tools are indispensable for scanning large numbers of machines, Scapy is like a fine-grained scalpel for manipulating a single target in a myriad of cool ways. With all kinds of features, Scapy just rocks. In ... [Continue reading Scapy Cheat Sheet from SANS SEC560](#)

On the right side of the page, there are social media sharing buttons for 8+1, Tweet, Like, and Share. Below these is a search bar and a "Categories" section with a list of tags:

- Anomaly Analysis (1)
- Anti-Virus Evasion (7)
- Backdoor (2)
- Challenges (25)
- Cheatsheet (2)
- cloud (1)
- Conferences (4)
- Cryptography (4)
- CyberCity (1)
- Databases (1)
- Enumeration (2)
- Exploit Development (4)
- File Analysis (1)
- fuzzing (1)
- Infrastructure (3)
- Introduction (2)
- Legal Issues (1)
- Linux (1)
- Metasploit (7)
- Methodology (42)
- Mobile (18)
- Network Devices (3)
- Nmap (2)
- Passwords (6)
- Post Exploitation (10)
- PowerShell (1)
- Presentations (9)
- Protocol Analysis (1)
- Python (11)

FireEye Blogs

The screenshot shows a web browser displaying the FireEye blog post "RED TEAM TOOL ROUNDUP" dated July 27, 2016, by Evan Pena, Chris King, and Christopher Truncer. The page includes a navigation menu, a breadcrumb trail, and a "SIGN UP FOR EMAIL UPDATES" form with fields for First Name, Last Name, and Email Address, and checkboxes for "Executive Perspective Blog", "Threat Research Blog", and "Products and Services Blog". A "Subscribe" button is also present. On the right side, there are social media icons for LinkedIn, Twitter, Facebook, and Google+. Below the main text, there is a section titled "Domain Enumeration" with a link to a GitHub repository for ADEnumerator. A terminal window is shown with the following commands and output:

```

C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\User1>runas /netonly /user:corp\Peter.Parker powershell
Enter the password for corp\Peter.Parker:
Attempting to start powershell as user "corp\Peter.Parker" ...

C:\Users\User1>runas /netonly /user:corp\Peter.Parker powershell

powershell (running as corp\Peter.Parker)
PS C:\Windows\system32> $users = [adsisearcher]"LDAP://ou=Standard,ou=Users,ou=PenTestLab,DC=corp,DC=hackerplaypen,DC=com"
PS C:\Windows\system32> $users.Children

distinguishedName : <CN=Barbara Gordon,OU=Standard,OU=Users,OU=PenTestLab,DC=corp,DC=hackerplaypen,DC=com>
Path                : LDAP://CN=Barbara Gordon,ou=Standard,ou=Users,ou=PenTestLab
    
```

Cybrary

The screenshot shows the Cybrary website interface. At the top, there is a navigation bar with links for 'MY PROFILE', 'COURSES', 'OP3N', 'EXPLORE', 'TEAMS', and 'ADVERTISE'. A search bar and a user greeting 'Welcome, Rich' are also visible. The main content area is titled 'Published Cyber Security Blog Posts' and features three articles:

- [Product Update] Introducing Cybrary Teams**
Published: July 27, 2016 | By: TREVORH | Views: 55
Cybrary has been working hard to release our newest platform for individuals, allowing them to learn and develop their cyber security skills on Cybrary together. Drum-roll, please...Introducing Cybrary Teams! With Cybrary eclipsing the 500,000 Registered Users mark, we sought to find a way to bring people closer together to learn, share, and grow beyond what's currently available on Cybrary. We believe Cybrary Teams will be able to meet the needs of learning cohorts, IT/Security Teams, ... Continue Reading >>
- Juliar: A Misunderstood and Underutilized Language**
Published: July 26, 2016 | By: ginasilvertree | Views: 481
By Andrey Makhanov A lot of people think Juliar is a combination of Julia and R programming languages. However, that's simply not true. I originally created the *Juliar* programming language for a girl I used to love. She is a very talented artist and really wanted to find a way to express herself. She bought many books, and she wanted to learn how to create things on a computer. However, it proved difficult for her to understand the books, let alone the languages. I shared her pain. Whe ... Continue Reading >>
- Tradecraft Tuesday – Fuzzing for Vulnerabilities**
Published: July 26, 2016 | By: kylehan slovan | Views: 317
What is Tradecraft Tuesday? Every Tuesday at 12pm ET, Chris Bisnett and Kyle Hanslovan expose the techniques used by hackers. With their 20 combined years in offensive cyber security and digital forensics, Chris and Kyle cover a new topic each week in a LIVE video chat. These unrehearsed conversations allow anyone to learn, ask questions, and share their experiences from offensive and defensive perspectives. In case you miss an episode, each recorded session are uploaded to Cybrary's ... Continue Reading >>

On the left side of the page, there is a social sharing section titled 'Enjoy this Blog? Share now!' with icons for Facebook, Twitter, Google+, LinkedIn, and Email.

Hacker News

The screenshot shows the Hacker News website interface. At the top, there is a navigation bar with links for Home, Hacking, Tech, Cyber Attacks, Vulnerabilities, Malware, and Spying. The main header features the site's logo, "The Hacker News Security in a serious way", and social media statistics for Google+, Twitter, and Facebook. Below the header, there are three product listings: a Supermicro SuperServer 5038D-I, 2FA Endpoint Protection by duo.com, and an Hp 813874-B21 10Gbase-T Sfp+ Transceiver. The main content area features two articles. The first article, "End of SMS-based 2-Factor Authentication; Yes, It's Insecure!", is dated Wednesday, July 27, 2016, by Mohit Kumar and has 63 Google+ likes, 1.1K Facebook likes, 2157 shares, 314 tweets, 21 LinkedIn shares, and 2560 general shares. It includes a red banner with the text "SMS two-factor is Dead!" and an image of a hand holding a smartphone. The second article, "KeySniffer Lets Hackers Steal Keystrokes from Wireless Keyboards", is also dated Wednesday, July 27, 2016, by Mohit Kumar and has 19 Google+ likes, 1K Facebook likes, 699 shares, 89 tweets, 12 LinkedIn shares, and 810 general shares. It includes a graphic with the text "KeySniffer" and "All your keystrokes, passwords, credit card numbers and everything you type are readable to anyone". To the right of the articles, there is a green advertisement for "ALIEN VAULT" titled "Beginner's Guide to Open Source Intrusion Detection Tools" with a "DOWNLOAD FREE GUIDE" button. Below the advertisement, there is a partial view of the Supermicro SuperServer 5038D-I - 4x... article, which includes an image of the server hardware.

Housekeeping



Housekeeping

1. Send me your student survey & agreement today.
2. Lab 1 due by 11:59PM (Opus time) tonight.
3. Last day to drop/add is this Saturday.

Change your default password on Opus

Roll Call

If you are attending class by watching the recordings in the archives email the instructor at: risimms@cabrillo.edu to provide roll call attendance.

Navigating SANS Pen Test Cheat Sheets for Fun and Profit

Thursday, September 8th, 2016 at 11:00 AM (11:00:00 EDT/US Eastern)

Ed Skodis

You can now attend the webcast using your mobile device!



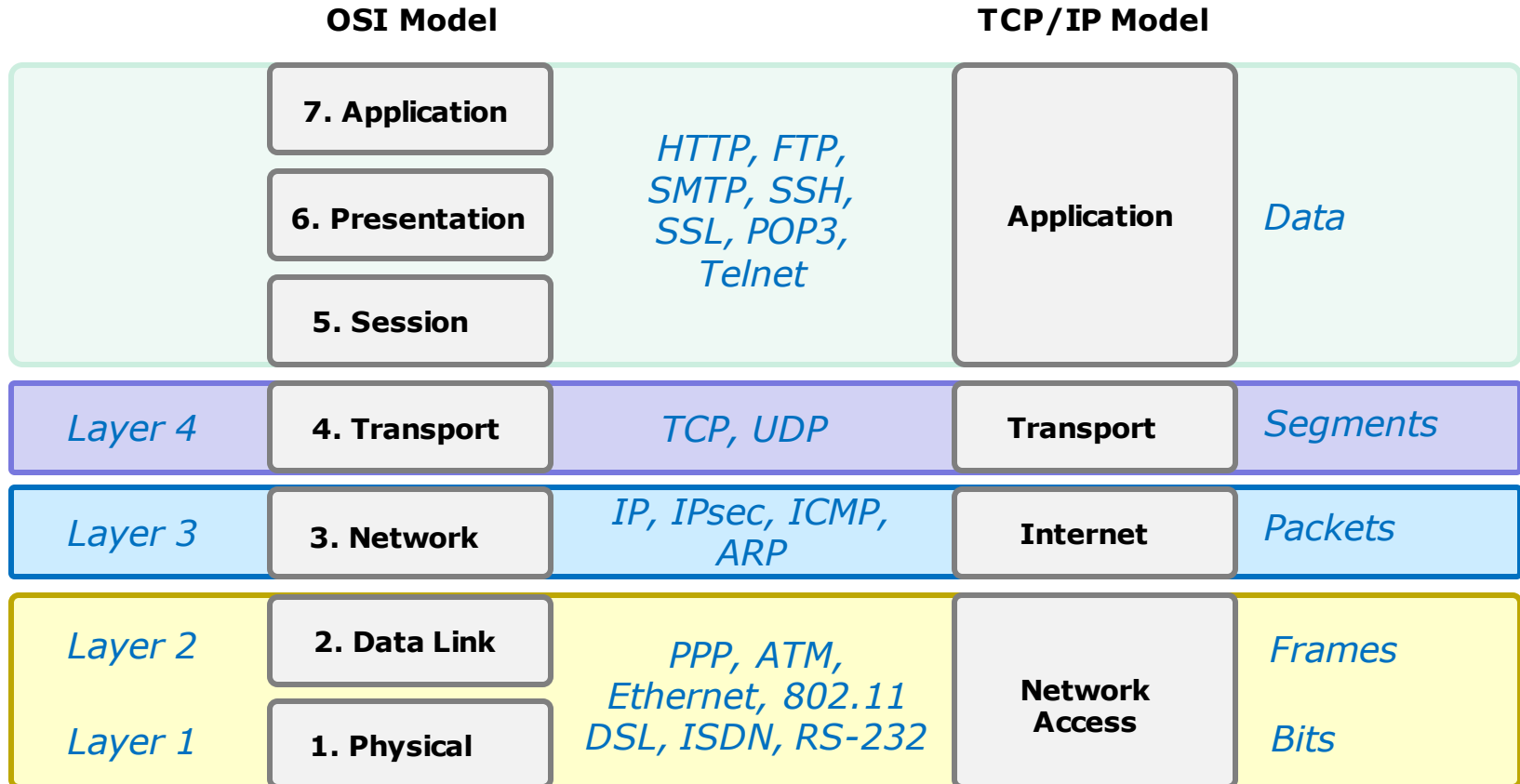
Overview

Extra! Extra! Get yer SANS Pen Test cheat sheets here! As you may have noticed, SANS Pen Test Authors and Instructors have been on a tear lately, releasing numerous cheat sheets to help people build valuable skills. Recent releases include topics such as PowerShell, Scapy, Nmap, Metasploit, and a whole bunch more. In this engaging webcast, Ed Skoudis will take you on a tour of some of the most useful tips and ideas of these cheat sheets. Five essential things to know about PowerShell? We got that. The most useful Scapy options at a glance? Got that too. The syntax for Netcat client-to-client relays? Yep. Some late-breaking Metasploit kung fu? Oh yes. Well also look at ways you can use the cheat sheets in your work and we might even go over some useful origami tricks. Ed will also solicit ideas from you on new cheat sheets you'd like to see.

https://www.sans.org/webcasts/navigating-pen-test-cheat-sheets-fun-profit-102897?utm_medium=Email&utm_source=House+List&utm_content=Navigating+Pen+Test+Cheat+Sheets&utm_campaign=SANS+Webcast+Internal

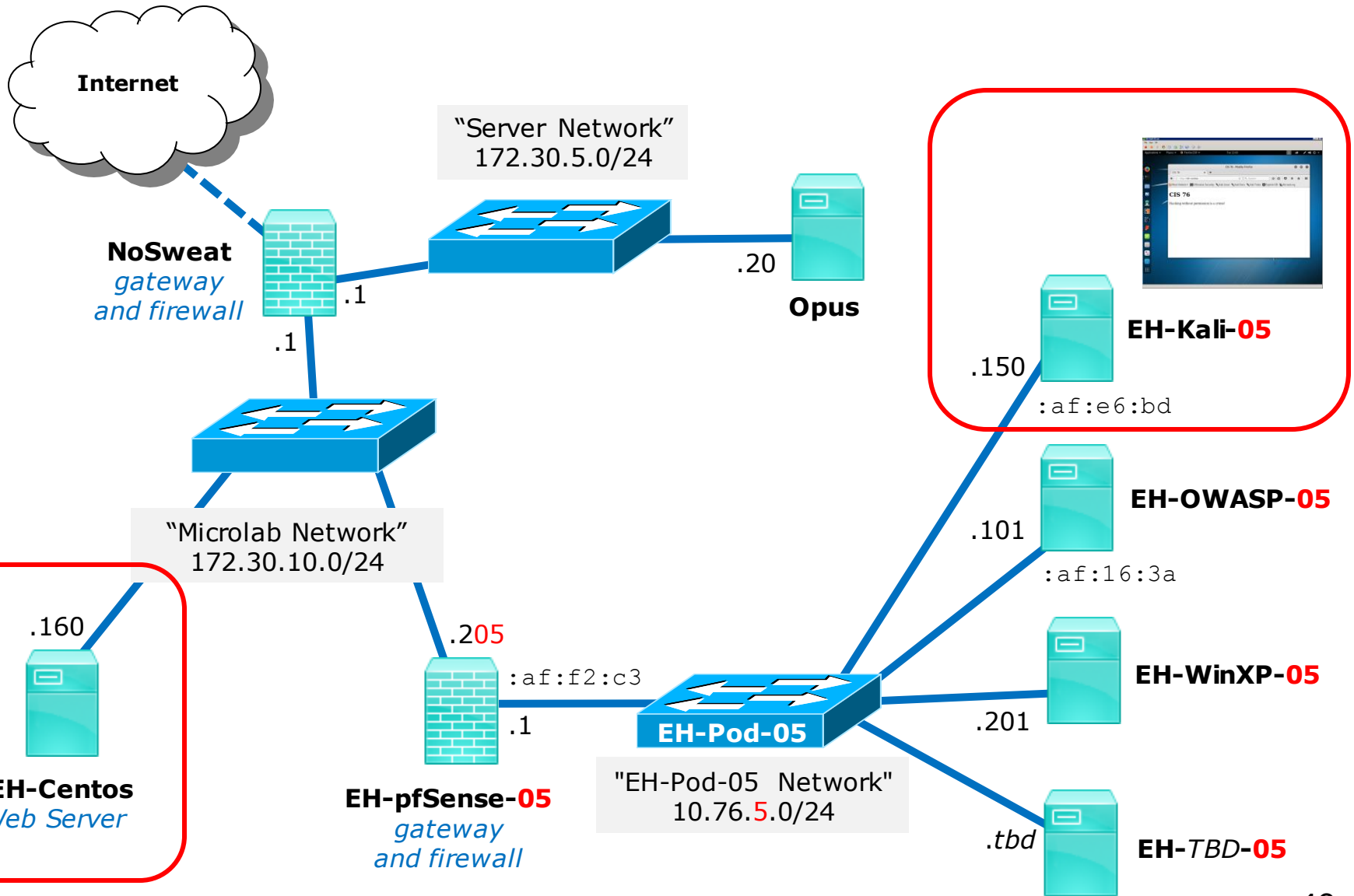
TCP/IP Review

OSI and TCP/IP Models



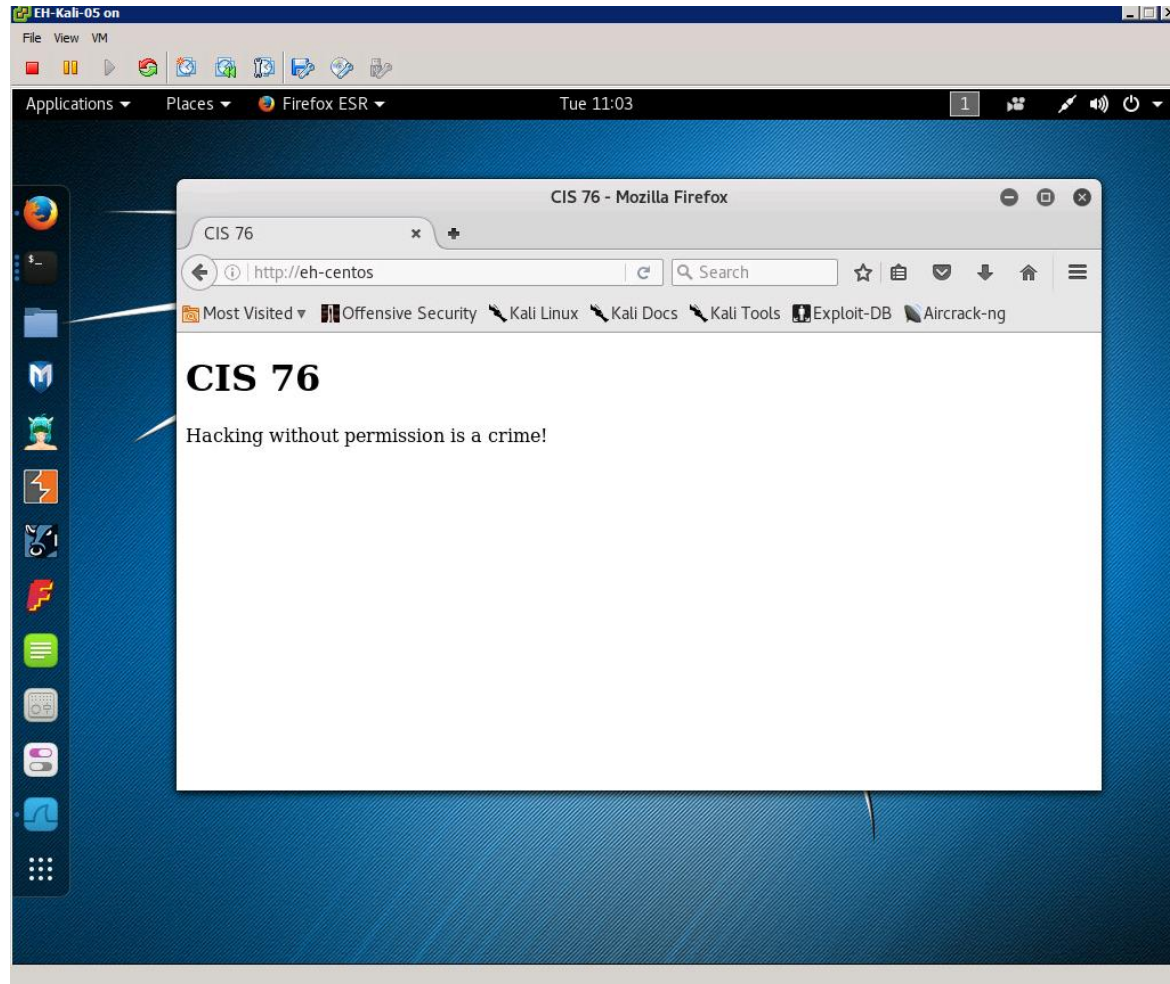
*Open Systems
Interconnection model*

*Model used to
build the Internet*

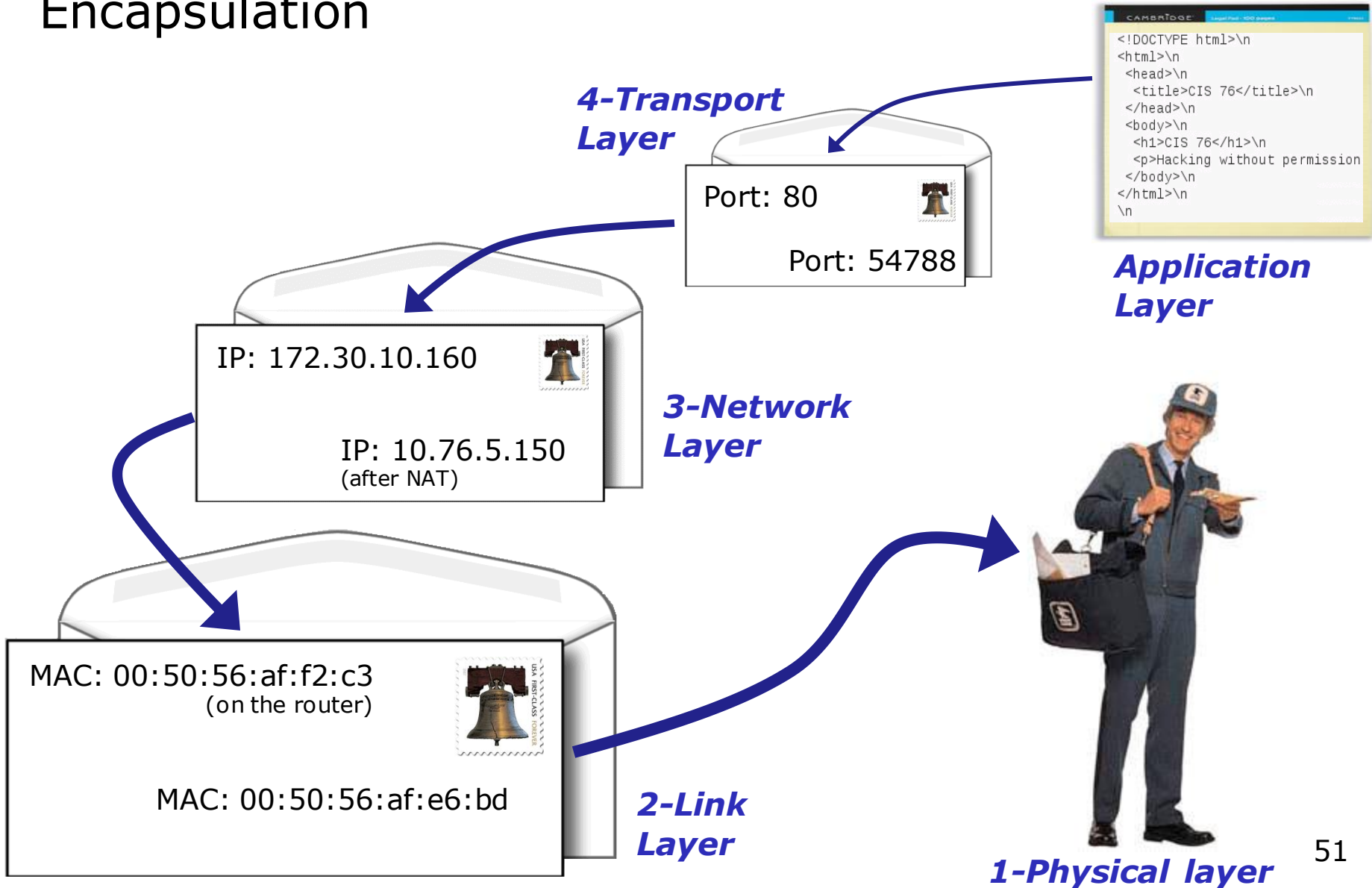


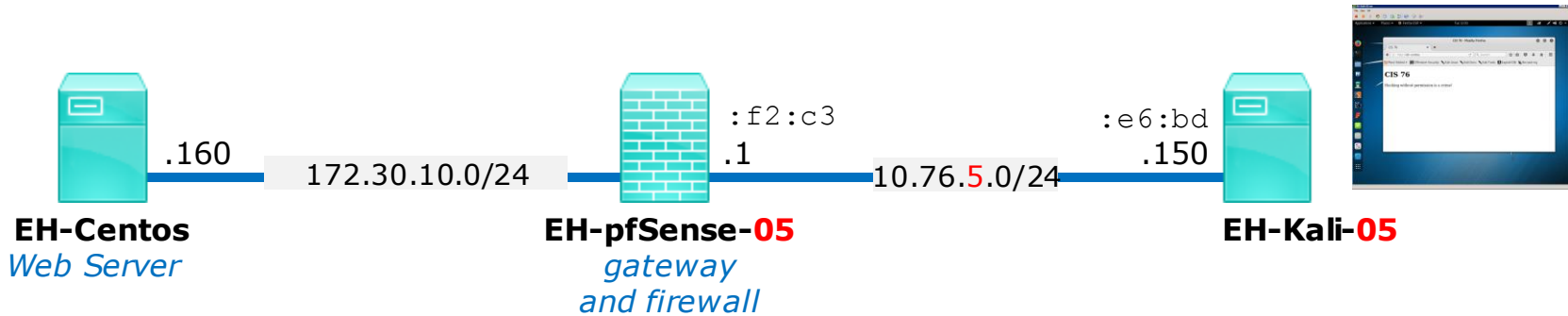
HTTP Application Example

Kali browsing a web page on EH-Centos



Encapsulation





No.	Time	Source	Destination	Protocol	Leng	Info
41	19.321087319	10.76.5.150	172.30.10.160	HTTP	68	GET / HTTP/1.0
43	19.322348239	172.30.10.160	10.76.5.150	HTTP	490	HTTP/1.1 200 OK (text/html)


```

▶ Frame 43: 490 bytes on wire (3920 bits), 490 bytes captured (3920 bits) on interface 0
▼ Ethernet II, Src: Vmware_af:f2:c3 (00:50:56:af:f2:c3), Dst: Vmware_af:e6:bd (00:50:56:af:e6:bd)
  ▶ Destination: Vmware_af:e6:bd (00:50:56:af:e6:bd)
  ▶ Source: Vmware_af:f2:c3 (00:50:56:af:f2:c3)
  Type: IPv4 (0x0800)
▶ Internet Protocol Version 4, Src: 172.30.10.160, Dst: 10.76.5.150
▶ Transmission Control Protocol, Src Port: 80 (80), Dst Port: 54788 (54788), Seq: 1, Ack: 19, Len: 424
▶ Hypertext Transfer Protocol
▼ Line-based text data: text/html
<!DOCTYPE html>\n
<html>\n
<head>\n
  <title>CIS 76</title>\n
</head>\n
<body>\n
  <h1>CIS 76</h1>\n
  <p>Hacking without permission is a crime!</p>\n
</body>\n
</html>\n
\n
  
```

Wireshark View On Kali

Wireshark Follow TCP Stream View On Kali

The screenshot shows the Wireshark interface with the 'Follow TCP Stream' window open for 'tcp.stream eq 3'. The window displays the following details:

```

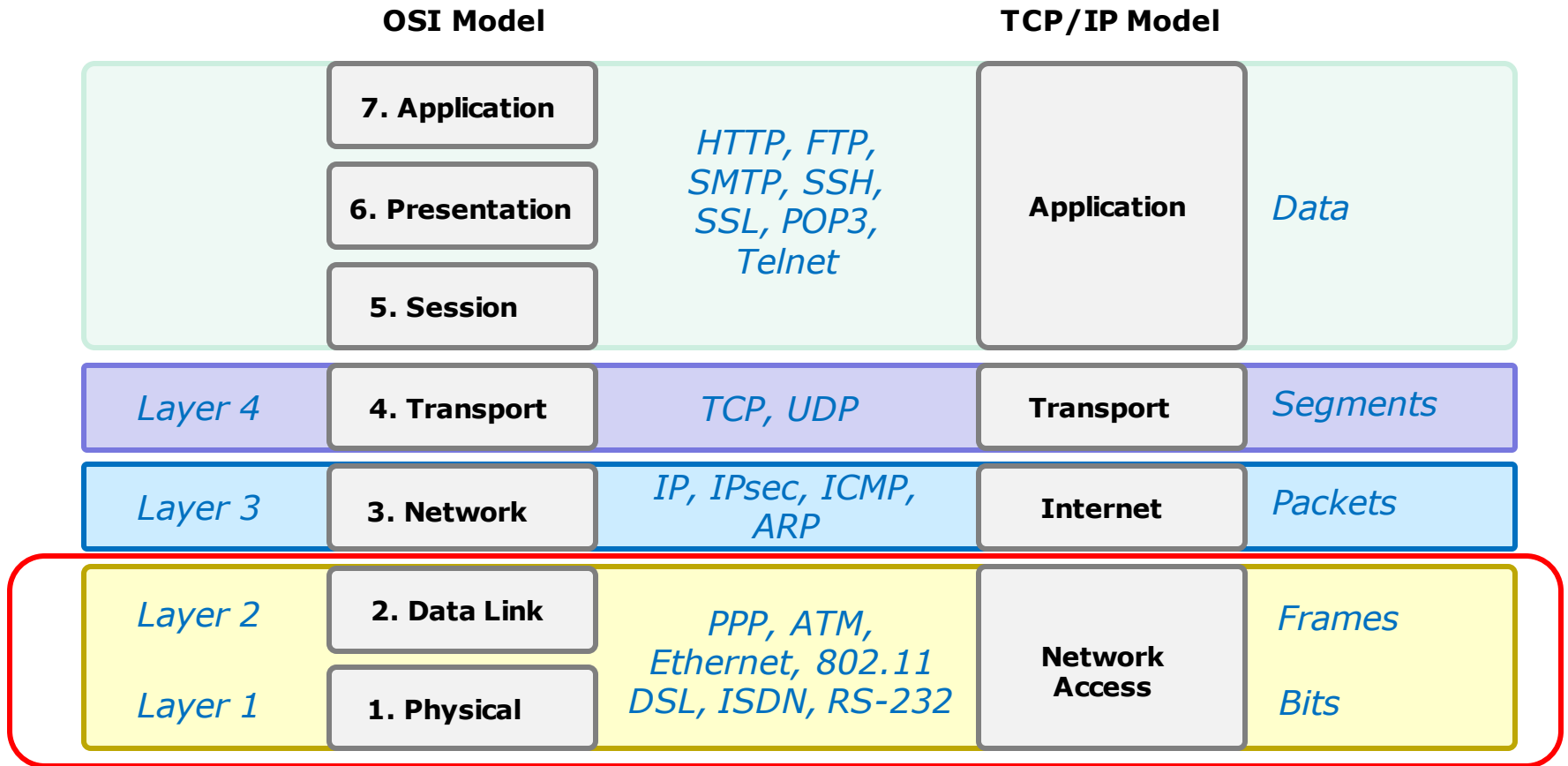
HTTP/1.1 200 OK
Date: Tue, 06 Sep 2016 02:24:27 GMT
Server: Apache/2.2.15 (CentOS)
Last-Modified: Fri, 02 Sep 2016 19:20:24 GMT
ETag: "22044-9c-53b8b38e1949a"
Accept-Ranges: bytes
Content-Length: 156
Connection: close
Content-Type: text/html; charset=UTF-8

<!DOCTYPE html>
<html>
<head>
<title>CIS 76</title>
</head>
<body>
<h1>CIS 76</h1>
<p>Hacking without permission is a crime!</p>
</body>
</html>
  
```

Below the HTML content, the 'GET / HTTP/1.0' request is visible. The packet list on the left shows frames 19 through 44, with frame 43 selected. The packet details pane on the right shows the 'Hypertext Transfer Protocol' section with a length of 424 bytes.

Network Access Layer

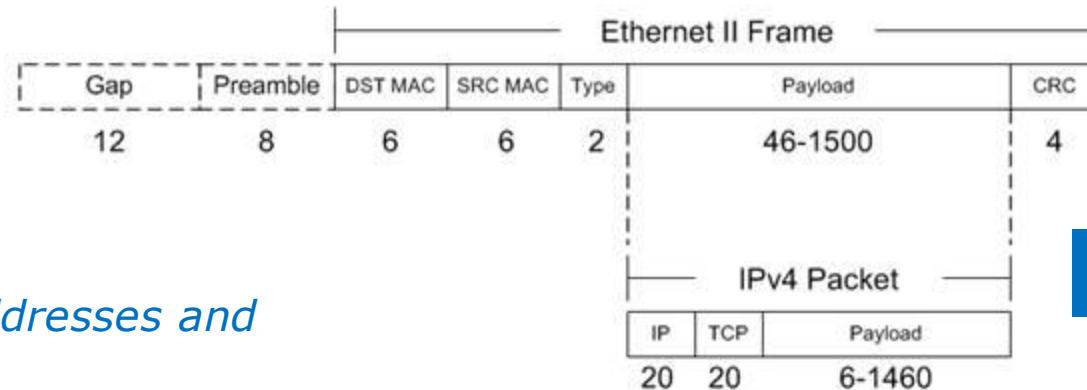
OSI and TCP/IP Models



*Open Systems
Interconnection model*

*Model used to
build the Internet*

Lets start at the bottom



<http://www.tamos.net/~rhay/overhead/ip-packet-overhead.htm>

Note the MAC addresses and type of payload

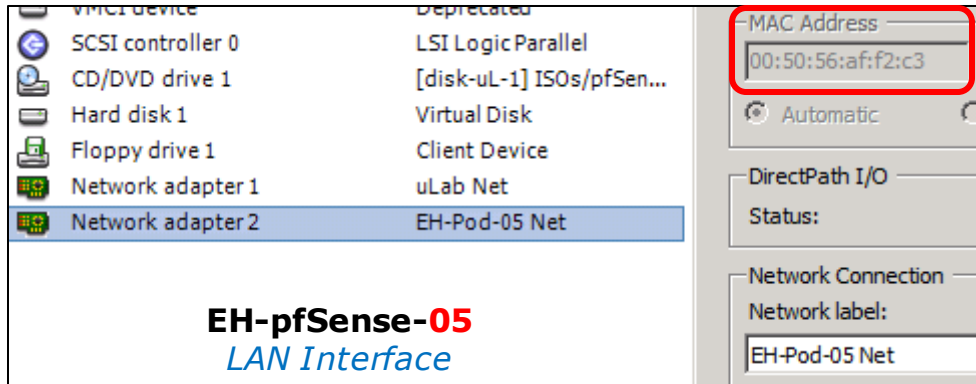
No.	Time	Source	Destination	Protocol	Leng	Info
41	19.321087319	10.76.5.150	172.30.10.160	HTTP	68	GET / HTTP/1.0
43	19.322348239	172.30.10.160	10.76.5.150	HTTP	490	HTTP/1.1 200 OK (text/html)

▶	Frame 43: 490 bytes on wire (3920 bits), 490 bytes captured (3920 bits) on interface 0
▼	Ethernet II, Src: Vmware_af:f2:c3 (00:50:56:af:f2:c3), Dst: Vmware_af:e6:bd (00:50:56:af:e6:bd)
▶	Destination: Vmware_af:e6:bd (00:50:56:af:e6:bd)
▶	Source: Vmware_af:f2:c3 (00:50:56:af:f2:c3)
▶	Type: IPv4 (0x0800)
▶	Internet Protocol Version 4, Src: 172.30.10.160, Dst: 10.76.5.150
▶	Transmission Control Protocol, Src Port: 80 (80), Dst Port: 54788 (54788), Seq: 1, Ack: 19, Len: 424
▶	Hypertext Transfer Protocol
▶	Line-based text data: text/html

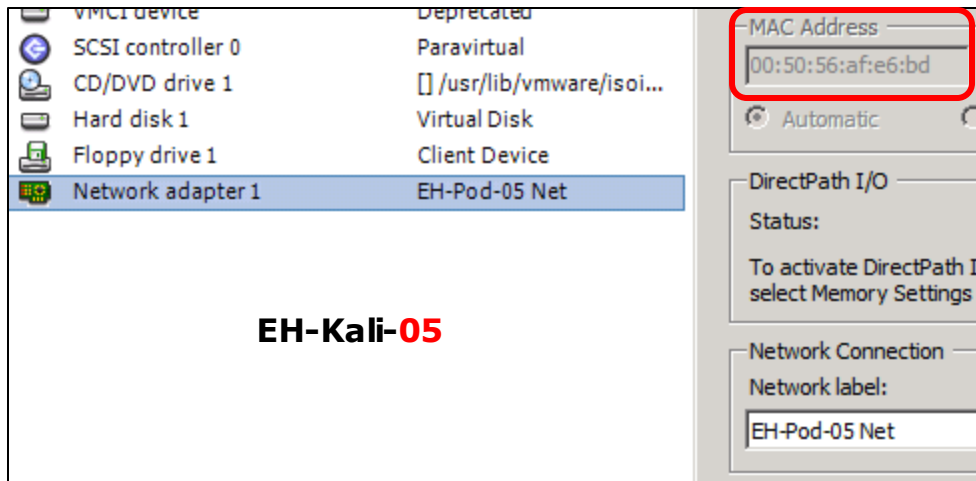
Layer 2 - Ethernet MAC Address

- Layer 2 defines how the streams of bits are organized into frames.
- In Ethernet each frame has a source and destination MAC address.
- MAC (Media Access Control) addresses came from the original Xerox Ethernet addressing scheme.
- A MAC address has 48 bits (6 octets).
 - e.g. 00:50:56:af:e6:bd
 - Note the use of hexadecimal digits to specify the octets.
- First three octets are the OUI (Organizationally Unique Identifier).
- Last three octets are unique to the NIC (Network Interface Controller).

Layer 2 - Ethernet MAC Addresses on VMs



00:50:56:af:f2:c3



00:50:56:af:e6:bd

Use "Edit Settings" to view MAC addresses on the network adapters

<https://www.wireshark.org/tools/oui-lookup.html>

There are many MAC Lookup tools available on the Internet to identify the company producing the network device

<https://www.wireshark.org/tools/oui-lookup.html>

OUI search

00:50:56:af:e6:bd

Find

Results

00:50:56 VMware, Inc.

OUI Lookup Tool
The Wireshark OUI lookup tool provides an easy way to look up OUIs and other MAC address prefixes. It uses the [Wireshark manufacturer database](#), which is a list of OUIs and MAC addresses compiled from a number of sources.

Directions:
Type or paste in a list of OUIs, MAC addresses, or descriptions below. OUIs and MAC addresses may be colon-, hyphen-, or period-separated.

Examples:
0000.0c
08:00:20
01-00-0C-CC-CC-CC
missouri

OUI search
00:50:56:af:e6:bd

Find

Results
00:50:56 VMware, Inc.

No.	Time	Source	Destination	Protocol	Length	Info
→ 1	0.000000000	10.76.5.150	10.76.5.1	ICMP	98	Echo (ping) request id=0x1f77, seq=1/256,
← 2	0.000379456	10.76.5.1	10.76.5.150	ICMP	98	Echo (ping) reply id=0x1f77, seq=1/256,


```

▶ Frame 1: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface 0
▼ Ethernet II, Src: Vmware_af:e6:bd (00:50:56:af:e6:bd), Dst: Vmware_af:f2:c3 (00:50:56:af:f2:c3)
  ▶ Destination: Vmware_af:f2:c3 (00:50:56:af:f2:c3)
  ▶ Source: Vmware_af:e6:bd (00:50:56:af:e6:bd)
    Type: IPv4 (0x0800)
▶ Internet Protocol Version 4, Src: 10.76.5.150, Dst: 10.76.5.1
▶ Internet Control Message Protocol
    
```

EH-pfSense-05 NIC (points to Destination MAC)

EH-Kali-05 NIC (points to Source MAC)

wireshark_pcapng_eth0_20160903151049_5BfPkm Packets: 2 · Displayed: 2 (100.0%) Profile: Default

```

root@eh-kali-05: ~
File Edit View Search Terminal Help
root@eh-kali-05:~# ping -c1 10.76.5.1
PING 10.76.5.1 (10.76.5.1) 56(84) bytes of data:
64 bytes from 10.76.5.1: icmp_seq=1 ttl=64 time=0.413 ms

--- 10.76.5.1 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.413/0.413/0.413/0.000 ms
root@eh-kali-05:~#
    
```

Pinging the pfSense VM from the Kali VM

Example Mac Address Filtering

ASUS RT-AC66U MAC Filtering

ASUS RT-AC66U Logout Reboot English

Operation Mode: **Wireless router** Firmware Version: **3.0.0.4.372.67** SSID: **ASUS ASUS_5G**

Firewall - MAC Filter

MAC filter allows you to accept or deny network access for devices with specific MAC addresses. You can set the MAC filter to the Accept or Reject mode. In the Reject mode, devices in the list are denied access to the network. In the Accept mode, only the devices that are in the list can access the network. The devices that are not in the list are denied access to the network.

Basic Config

MAC Filter Mode: **Disabled**

MAC filter list (Max Limit : 32)

MAC address	Add / Delete
	+

No data in table.

Apply

This router enables MAC address filtering to Accept or Reject MAC addresses

http://event.asus.com/2012/nw/dummy_ui/en/Advanced_MACFilter_Content.html

Example Mac Address Filtering

Cisco Aironet 1300 Series Outdoor Access Point

The screenshot shows the configuration page for MAC Address Filters on a Cisco Aironet 1300 Series Outdoor Access Point. The interface includes a navigation menu on the left, a breadcrumb trail at the top, and a main configuration area.

- Navigation Menu:** HOME, EXPRESS SET-UP, EXPRESS SECURITY, NETWORK MAP, ASSOCIATION, NETWORK INTERFACES, SECURITY, SERVICES (Telnet/SSH, CDP, DNS, Filters, HTTP, Proxy Mobile IP, QoS, SNMP, NTP, VLAN, STP, ARP Caching), WIRELESS SERVICES, SYSTEM SOFTWARE, EVENT LOG.
- Breadcrumb Trail:** APPLY FILTERS > MAC ADDRESS FILTERS > IP FILTERS > ETHERTYPE FILTERS.
- Host Information:** Hostname: bridge; bridge uptime is 1 day, 23 hours, 26 minutes.
- Services: Filters - MAC Address Filters:**
 - Create/Edit Filter Index:** < NEW >
 - Filter Index:** (700-799)
 - Add MAC Address:** (HHHH.HHHH.HHHH) **Mask:** 0000.0000.0000 (HHHH.HHHH.HHHH) **Action:** Forward Add
 - Default Action:** Block All
 - Filters Classes:** (Empty list with Delete Class button)
- Bottom Buttons:** Apply, Delete, Cancel.

Configuring address filters on a Cisco Access Point

http://www.cisco.com/c/en/us/td/docs/wireless/access_point/1300/12-3_7_JA/configuration/guide/brsc1237/b37filt.html

117028

MAC Address Spoofing

Layer 2 - MAC Address Spoofing

Why would a hacker do this?

- Create an anonymous identity for a network device.
- Impersonate another network device.
- Gain unauthorized access to services.
- Bypass access control lists that allow and block specific MAC addresses.

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

Live demo

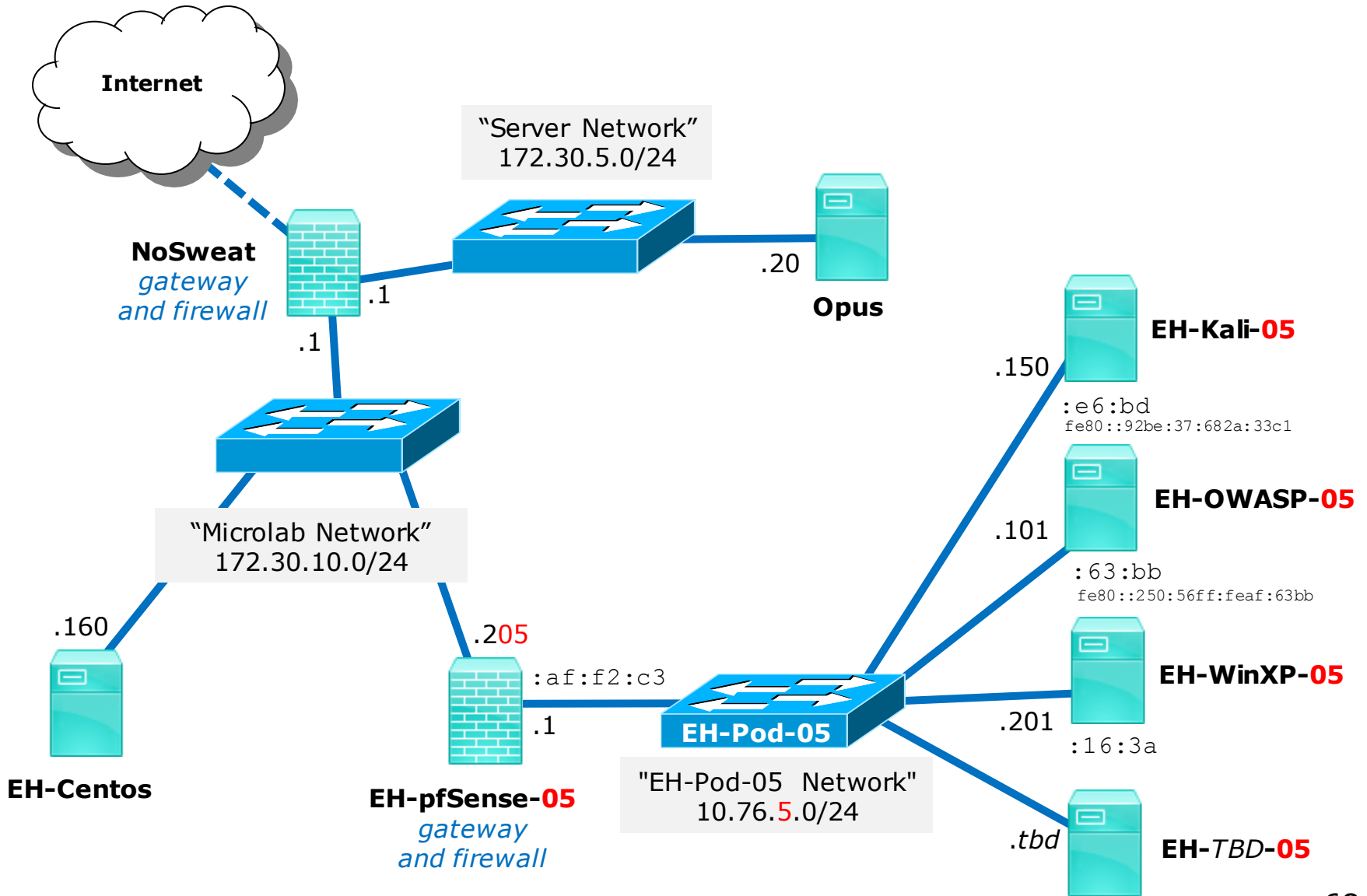
<https://simms-teach.com/docs/cis76/cis76-MAC-spoofing.pdf>

ARP

ARP - Address Resolution Protocol

- ARP uses layer 2 for transport but unlike IP has no headers and is not routable.
- Before an IP packet can be sent the sender needs to know the MAC address of either:
 - The destination device if it is on the same subnet.
 - The next-hop router if the destination is on a remote network.
- The sender "shouts out" (broadcasts) to the subnet "Who has such and such IP address"
- The IP address owner sends back (unicast) the MAC address.
- The sender can then encapsulate the IP packet into an Ethernet frame and send it to the appropriate MAC address.
- Devices will temporarily save IP/MAC pairs in an arp cache for reuse.
- ARP has been replaced by Neighbor Solicitation & Advertisement in IPv6.

<https://keepingitclassless.net/2011/10/neighbor-solicitation-ipv6s-replacement-for-arp/>



ARP Example - getting Kali VM MAC

WinXP VM requests the MAC address of the Kali VM before pinging

0.00000000	vmware_af:16:3a	Broadcast	ARP	42 who has 10.76.5.150? Tell 10.76.5.201
0.00029100	vmware_af:e6:bd	vmware_af:16:3a	ARP	60 10.76.5.150 is at 00:50:56:af:e6:bd
0.00030700	10.76.5.201	10.76.5.150	ICMP	74 Echo (ping) request id=0x0200, seq=3328/13, ttl=128 (r
0.00049900	10.76.5.150	10.76.5.201	ICMP	74 Echo (ping) reply id=0x0200, seq=3328/13, ttl=64 (re

WinXP Wireshark view

```

C:\WINDOWS\system32\cmd.exe
C:\>arp -a
No ARP Entries Found

C:\>ping 10.76.5.150

Pinging 10.76.5.150 with 32 bytes of data:

Reply from 10.76.5.150: bytes=32 time<1ms TTL=64
Reply from 10.76.5.150: bytes=32 time<1ms TTL=64
Reply from 10.76.5.150: bytes=32 time<1ms TTL=64
Reply from 10.76.5.150: bytes=32 time<1ms TTL=64

Ping statistics for 10.76.5.150:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>arp -a

Interface: 10.76.5.201 --- 0x2
    Internet Address      Physical Address      Type
    10.76.5.150           00-50-56-af-e6-bd    dynamic
  
```

Notice the arp cache is populated after the ping operation

WinXP command line

ARP Example - getting OWASP VM MAC

WinXP VM requests the MAC address of the OWASP VM before pinging

Time	Source	Destination	Protocol	Length	Info
0.00000000	vmware_af:16:3a	Broadcast	ARP	42	who has 10.76.5.101? Tell 10.76.5.201
0.00037300	vmware_af:63:bb	vmware_af:16:3a	ARP	60	10.76.5.101 is at 00:50:56:af:63:bb
0.00039000	10.76.5.201	10.76.5.101	ICMP	74	Echo (ping) request id=0x0200, seq=4352/17, ttl=128 (r
0.00052400	10.76.5.101	10.76.5.201	ICMP	74	Echo (ping) reply id=0x0200, seq=4352/17, ttl=64 (re

WinXP Wireshark view

```

C:\WINDOWS\system32\cmd.exe
C:\>arp -a
No ARP Entries Found

C:\>ping 10.76.5.101

Pinging 10.76.5.101 with 32 bytes of data:

Reply from 10.76.5.101: bytes=32 time<1ms TTL=64
Reply from 10.76.5.101: bytes=32 time<1ms TTL=64
Reply from 10.76.5.101: bytes=32 time<1ms TTL=64
Reply from 10.76.5.101: bytes=32 time<1ms TTL=64

Ping statistics for 10.76.5.101:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>arp -a

Interface: 10.76.5.201 --- 0x2
Internet Address      Physical Address      Type
10.76.5.101           00-50-56-af-63-bb    dynamic
    
```

Notice the arp cache is populated after the ping operation

WinXP command line

ICMPv6 Neighbor Solicitation Example

Kali getting OWASP VM MAC

Kali Wireshark view

No.	Time	Source	Destination	Protocol	Leng	Info
2	60.048792053	fe80::92be:37:6...	ff02::1:ffaf:63bb	ICMPv6	86	Neighbor Solicitation for fe80::250:56ff:f...
3	60.049136713	fe80::250:56ff:...	fe80::92be:37:68...	ICMPv6	86	Neighbor Advertisement fe80::250:56ff:feaf...
4	60.049155306	fe80::92be:37:6...	fe80::250:56ff:f...	ICMPv6	118	Echo (ping) request id=0x5691, seq=1, hop ...
5	60.049331414	fe80::250:56ff:...	fe80::92be:37:68...	ICMPv6	118	Echo (ping) reply id=0x5691, seq=1, hop li...
6	61.049723000	fe80::92be:37:6...	fe80::250:56ff:f...	ICMPv6	118	Echo (ping) request id=0x5691, seq=2, hop ...
7	61.049953479	fe80::250:56ff:...	fe80::92be:37:68...	ICMPv6	118	Echo (ping) reply id=0x5691, seq=2, hop li...

▶ Frame 2: 86 bytes on wire (688 bits), 86 bytes captured (688 bits) on interface 0
 ▼ Ethernet II, Src: Vmware_af:e6:bd (00:50:56:af:e6:bd), Dst: IPv6mcast_ff:af:63:bb (33:33:ff:af:63:bb)
 ▶ Destination: **IPv6mcast_ff:af:63:bb (33:33:ff:af:63:bb)**
 ▶ Source: Vmware_af:e6:bd (00:50:56:af:e6:bd)
 Type: IPv6 (0x86dd)
 ▼ Internet Protocol Version 6, Src: fe80::92be:37:682a:33c1, Dst: **ff02::1:ffaf:63bb**
 0110 = Version: 6
 ▶ 0000 0000 = Traffic class: 0x00 (DSCP: CS0, ECN: Not-ECT)
 0000 0000 0000 0000 0000 0000 = Flowlabel: 0x00000000
 Payload length: 32
 Next header: ICMPv6 (58)
 Hop limit: 255
 Source: fe80::92be:37:682a:33c1
 Destination: ff02::1:ffaf:63bb
 [Source GeoIP: Unknown]
 [Destination GeoIP: Unknown]
 ▼ Internet Control Message Protocol v6
 Type: Neighbor Solicitation (135)
 Code: 0
 Checksum: 0xefd9 [correct]
 Reserved: 00000000
Target Address: fe80::250:56ff:feaf:63bb
 ▶ ICMPv6 Option (Source Link-Layer address : 00:50:56:af:e6:bd)

```

root@eh-kali-05:~# ping6 -c2 fe80::250:56ff:feaf:63bb
PING fe80::250:56ff:feaf:63bb(fe80::250:56ff:feaf:63bb) 56 data bytes
64 bytes from fe80::250:56ff:feaf:63bb%eth0: icmp_seq=1 ttl=64 time=0.233 ms
64 bytes from fe80::250:56ff:feaf:63bb%eth0: icmp_seq=2 ttl=64 time=0.402 ms

--- fe80::250:56ff:feaf:63bb ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 999ms
rtt min/avg/max/mdev = 0.233/0.317/0.402/0.086 ms
root@eh-kali-05:~# ip -6 neighbor show
fe80::250:56ff:feaf:63bb dev eth0 lladdr 00:50:56:af:63:bb REACHABLE
root@eh-kali-05:~#
  
```

Kali command line

Notice the multicast solicitation is asking for the MAC address of the OWASP VM

ICMPv6 Neighbor Advertisement Example

Kali getting OWASP VM MAC

Kali Wireshark view

No.	Time	Source	Destination	Protocol	Leng	Info
2	60.048792053	fe80::92be:37:6...	ff02::1:ffaf:63bb	ICMPv6	86	Neighbor Solicitation for fe80::250:56ff:f...
3	60.049136713	fe80::250:56ff:...	fe80::92be:37:68...	ICMPv6	86	Neighbor Advertisement fe80::250:56ff:feaf...
4	60.049155306	fe80::92be:37:6...	fe80::250:56ff:f...	ICMPv6	118	Echo (ping) request id=0x5691, seq=1, hop ...
5	60.049331414	fe80::250:56ff:...	fe80::92be:37:68...	ICMPv6	118	Echo (ping) reply id=0x5691, seq=1, hop li...
6	61.049723000	fe80::92be:37:6...	fe80::250:56ff:f...	ICMPv6	118	Echo (ping) request id=0x5691, seq=2, hop ...
7	61.049953479	fe80::250:56ff:...	fe80::92be:37:68...	ICMPv6	118	Echo (ping) reply id=0x5691, seq=2, hop li...


```

▶ Frame 3: 86 bytes on wire (688 bits), 86 bytes captured (688 bits) on interface 0
▼ Ethernet II, Src: Vmware_af:63:bb (00:50:56:af:63:bb), Dst: Vmware_af:e6:bd (00:50:56:af:e6:bd)
  ▶ Destination: Vmware_af:e6:bd (00:50:56:af:e6:bd)
  ▶ Source: Vmware_af:63:bb (00:50:56:af:63:bb)
  Type: IPv6 (0x86dd)
▼ Internet Protocol Version 6, Src: fe80::250:56ff:feaf:63bb, Dst: fe80::92be:37:682a:33c1
  0110 .... = Version: 6
  ▶ .... 0000 0000 .... = Traffic class: 0x00 (DSCP: CS0, ECN: Not-ECT)
  .... 0000 0000 0000 0000 0000 0000 = Flowlabel: 0x00000000
  Payload length: 32
  Next header: ICMPv6 (58)
  Hop limit: 255
  Source: fe80::250:56ff:feaf:63bb
  [Source SA MAC: Vmware_af:63:bb (00:50:56:af:63:bb)]
  Destination: fe80::92be:37:682a:33c1
  [Source GeoIP: Unknown]
  [Destination GeoIP: Unknown]
▼ Internet Control Message Protocol v6
  Type: Neighbor Advertisement (136)
  Code: 0
  Checksum: 0xb90f [correct]
  ▶ Flags: 0x60000000
  Target Address: fe80::250:56ff:feaf:63bb
  ▶ ICMPv6 Option (Target link-layer address : 00:50:56:af:63:bb)
  
```



```

root@eh-kali-05:~# ping6 -c2 fe80::250:56ff:feaf:63bb
PING fe80::250:56ff:feaf:63bb(fe80::250:56ff:feaf:63bb) 56 data bytes
64 bytes from fe80::250:56ff:feaf:63bb%eth0: icmp_seq=1 ttl=64 time=0.233 ms
64 bytes from fe80::250:56ff:feaf:63bb%eth0: icmp_seq=2 ttl=64 time=0.317 ms
--- fe80::250:56ff:feaf:63bb ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 999ms
rtt min/avg/max/mdev = 0.233/0.317/0.402/0.086 ms
root@eh-kali-05:~# ip -6 neighbor show
fe80::250:56ff:feaf:63bb dev eth0 lladdr 00:50:56:af:63:bb REACHABLE
root@eh-kali-05:~#
  
```

Notice the neighbor list on Kali is populated now

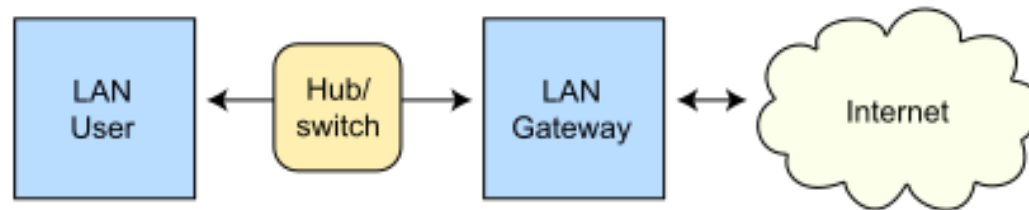
Kali command line

Notice the advertisement contains the OWASP MAC address

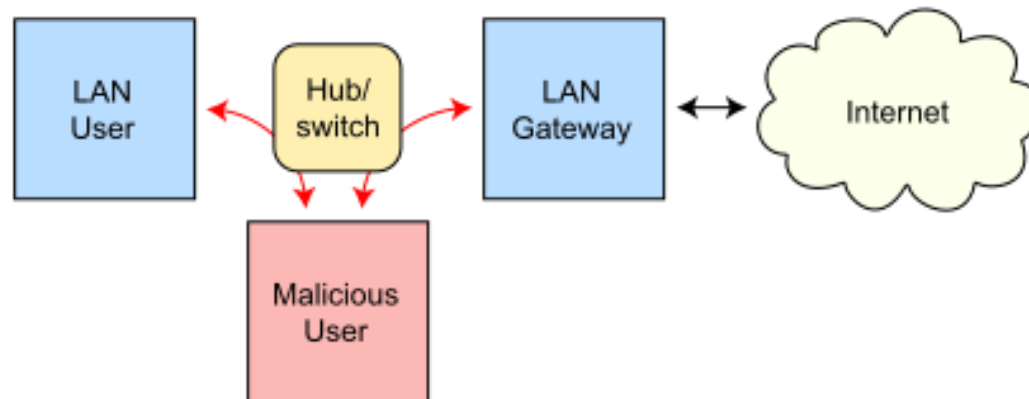
MITM attack using ARP Poisoning

Background on ARP Spoofing

Routing under normal operation



Routing subject to ARP cache poisoning



ARP Spoofing

Wikipedia article on ARP spoofing. The article title is "ARP spoofing" and the URL is "https://en.wikipedia.org/wiki/ARP_spoofing". The article text explains that ARP spoofing, also known as ARP cache poisoning or ARP poison routing, is a technique by which an attacker sends (spoofed) Address Resolution Protocol (ARP) messages onto a local area network. Generally, the aim is to associate the attacker's MAC address with the IP address of another host, such as the default gateway, causing any traffic meant for that IP address to be sent to the attacker instead.

ARP spoofing may allow an attacker to intercept data frames on a network, modify the traffic, or stop all traffic. Often the attack is used as an opening for other attacks, such as denial of service, man in the middle, or session hijacking attacks.^[1]

The attack can only be used on networks that use the Address Resolution Protocol, and is limited to local network segments.^[2]

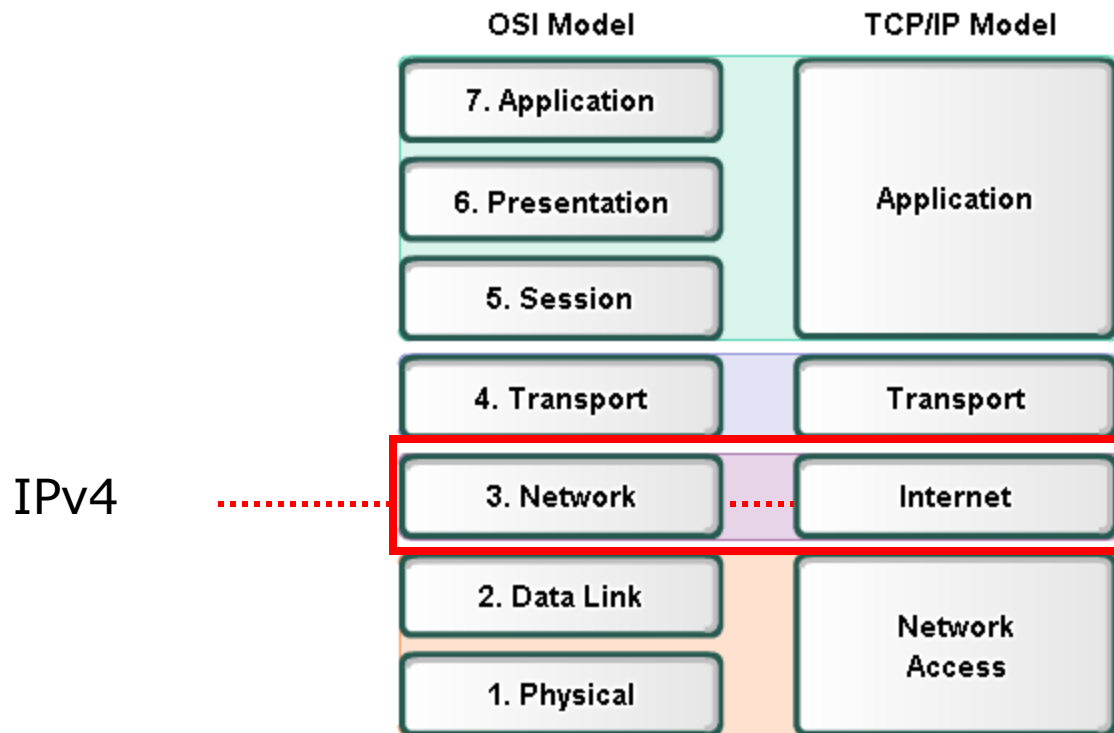
The diagram illustrates the difference between normal routing and routing subject to ARP cache poisoning. In normal operation, a LAN User connects to a Hub/Switch, which connects to a LAN Gateway, which then connects to the Internet. In the case of ARP cache poisoning, a Malicious User is introduced, and the Hub/Switch routes traffic from the LAN User to the Malicious User instead of the LAN Gateway.

Live demo

<https://simms-teach.com/docs/cis76/cis76-MITM-arp-poison.pdf>

Network Layer

Network Layer

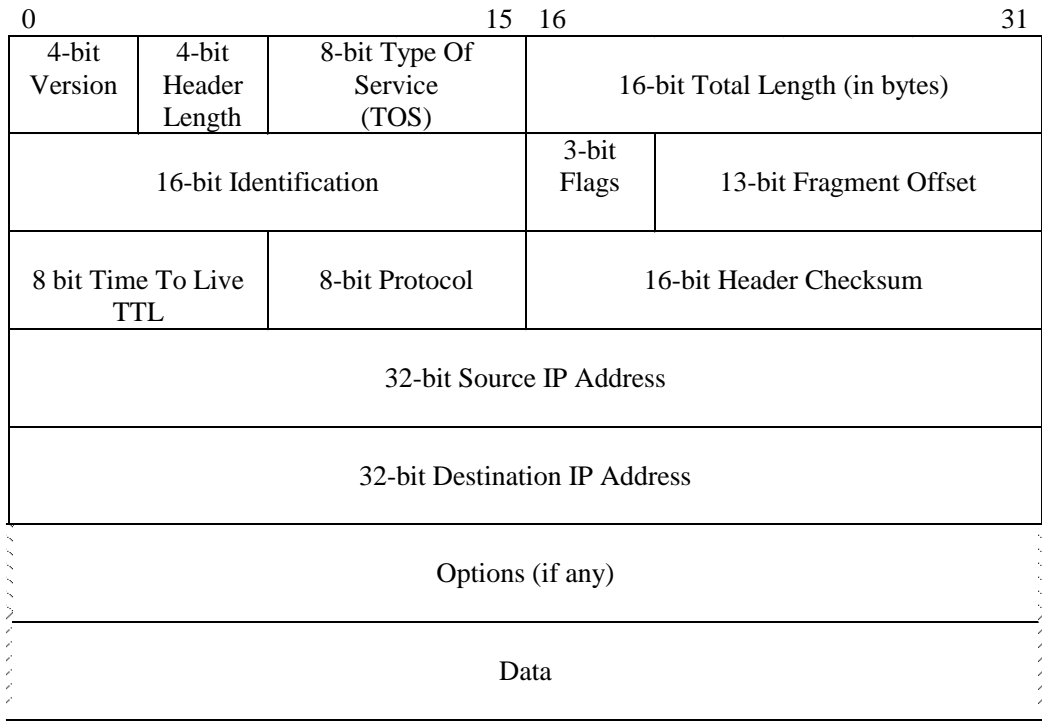


IPv4

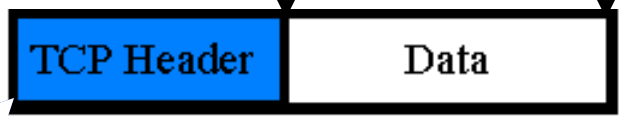
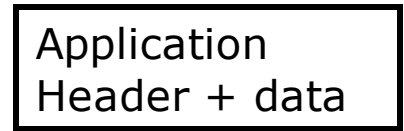
RS: More on Layer 3 tonight



CIS 76 - Lesson 2



IP Header



RS: showing how encapsulation works without the envelopes and postman this time

Addressing

192.168.100.99

Source IP = 192.168.100.99

Destination IP = 172.16.3.10



Source IP = 172.16.3.10

Destination IP = 192.168.100.99



172.16.3.10



- Source IP Address
- Destination IP Address
- More later!

RS: Layer 3 is where IP addresses are used. They are put in the header of the layer three packets.

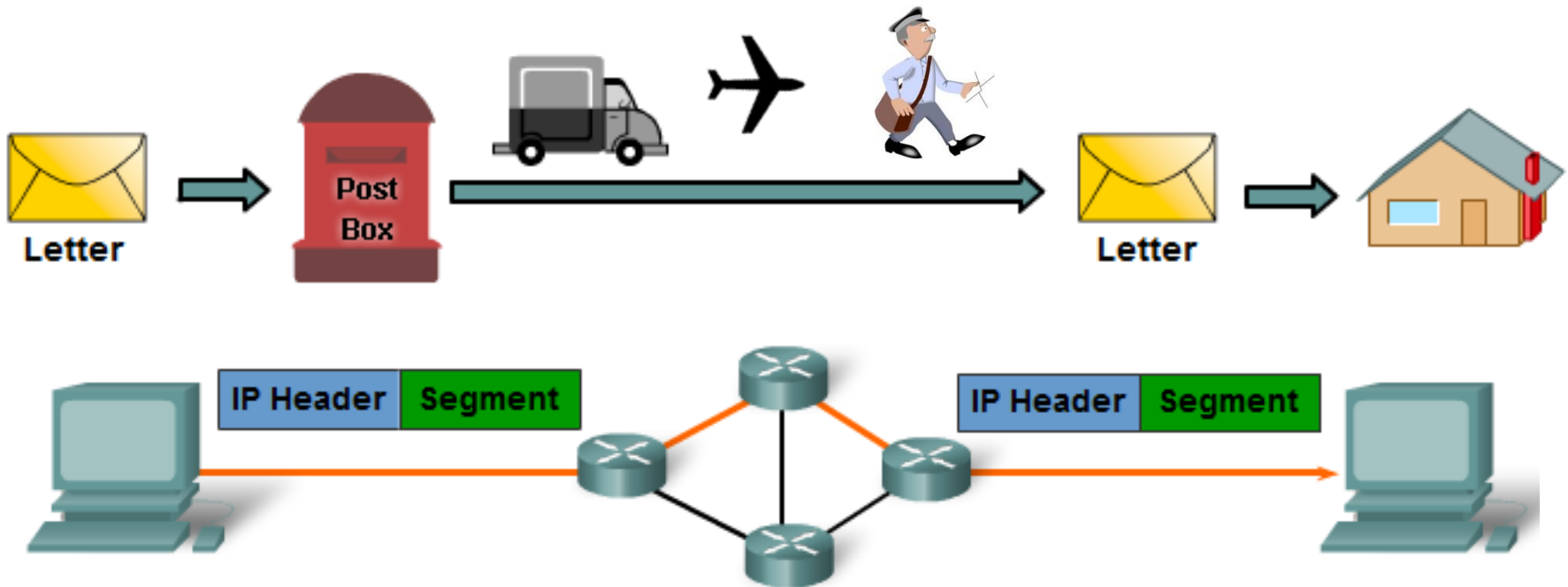


Network Layer Protocols

- Internet Protocol version 4 (IPv4)
- Internet Protocol version 6 (IPv6)
- Novell Internetwork Packet Exchange (IPX)
- AppleTalk
- Connectionless Network Service (CLNS/DECNet)

- The Internet Protocol (IPv4 and IPv6) is the most widely-used Layer 3 data carrying protocol and will be the focus of this course.

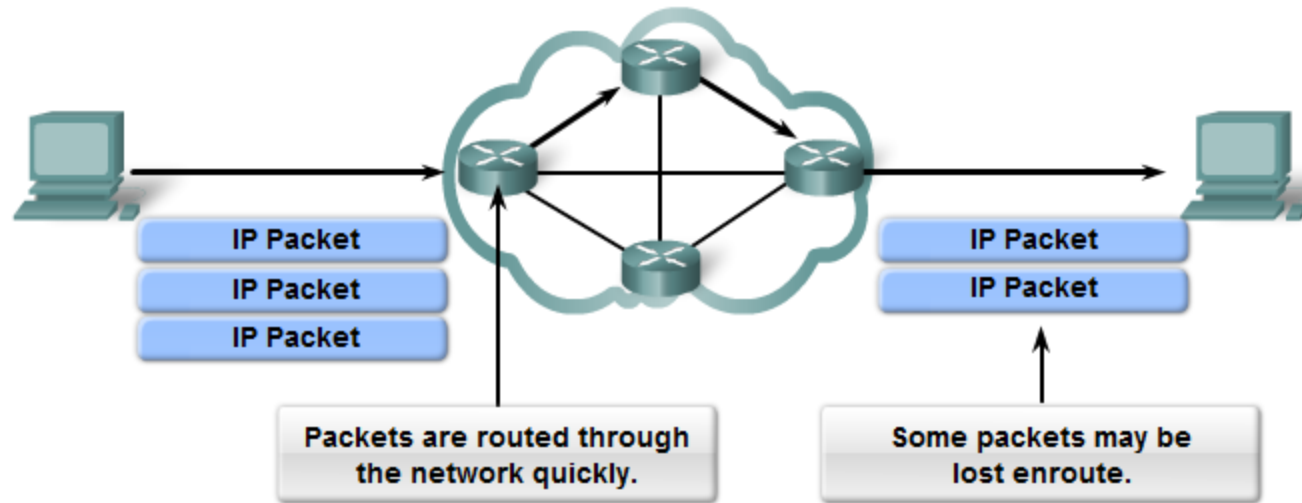
Connectionless



IP packets are sent without notifying the end host that they are coming. (*Layer 3*)

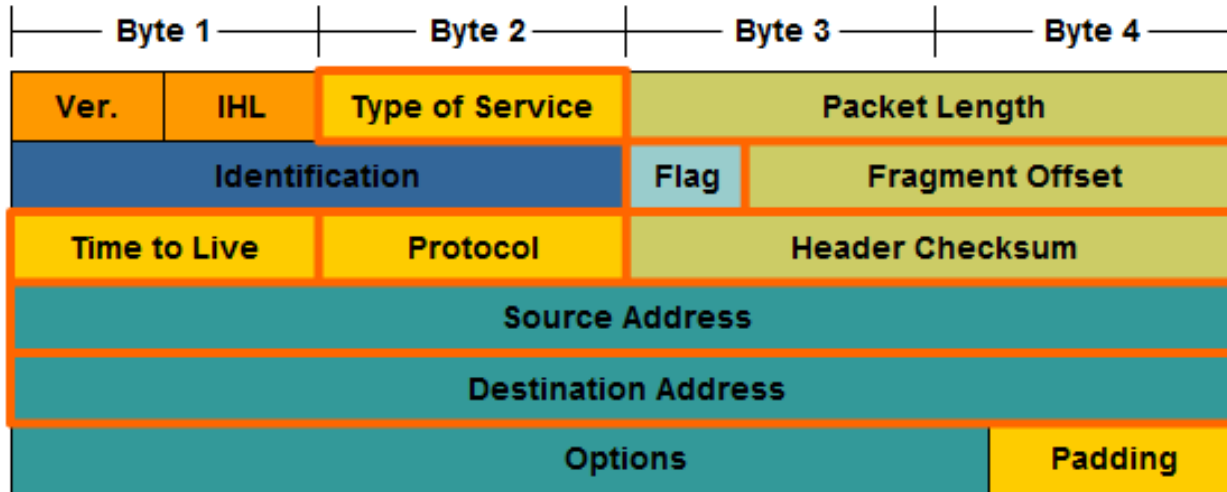
- **TCP**: A connection-oriented protocol does require a connection to be established prior to sending TCP segments. (*Layer 4*)
- **UDP**: A connectionless protocol does not require a session to be established. (*Layer 4*)

Best Effort Service (unreliable)



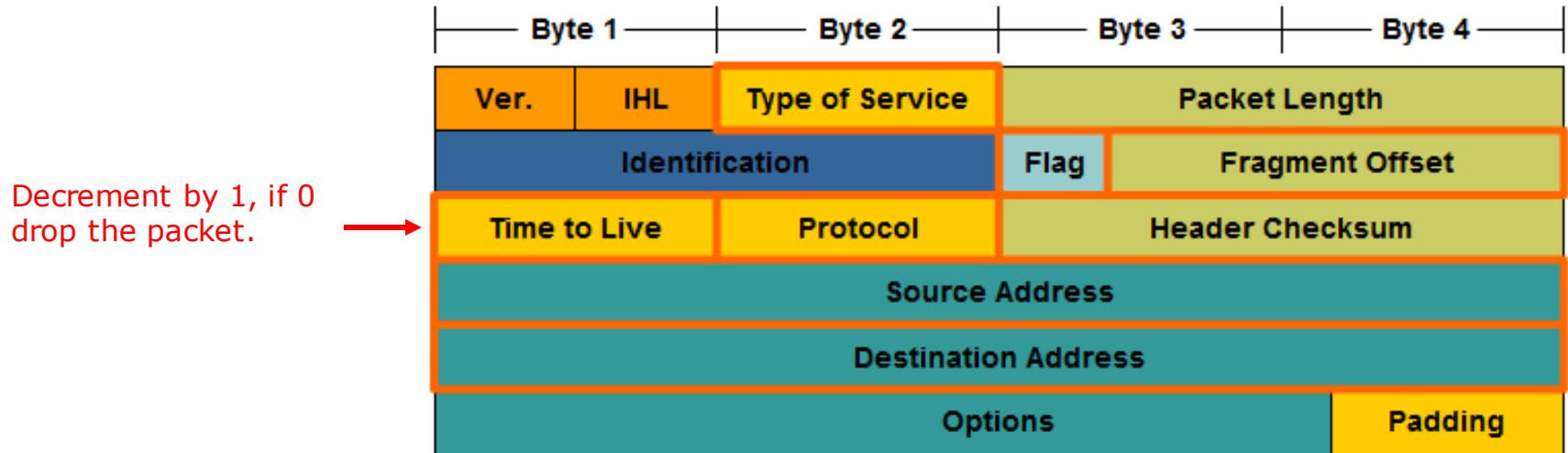
- The mission of Layer 3 is to transport the packets between the hosts while placing as little burden on the network as possible.
 - Speed over reliability
- Layer 3 is not concerned with or even aware of the type of data contained inside of a packet.
 - This responsibility is the role of the upper layers as required.
- **Unreliable:** IP does not have the capability or responsibility to manage or recover from, undelivered or corrupt packets.
 - TCP's responsibility at the end-to-end hosts

IP Header



- **IP Destination Address**
 - 32-bit binary value that represents the packet destination Network layer host address.
- **IP Source Address**
 - 32-bit binary value that represents the packet source Network layer host address.

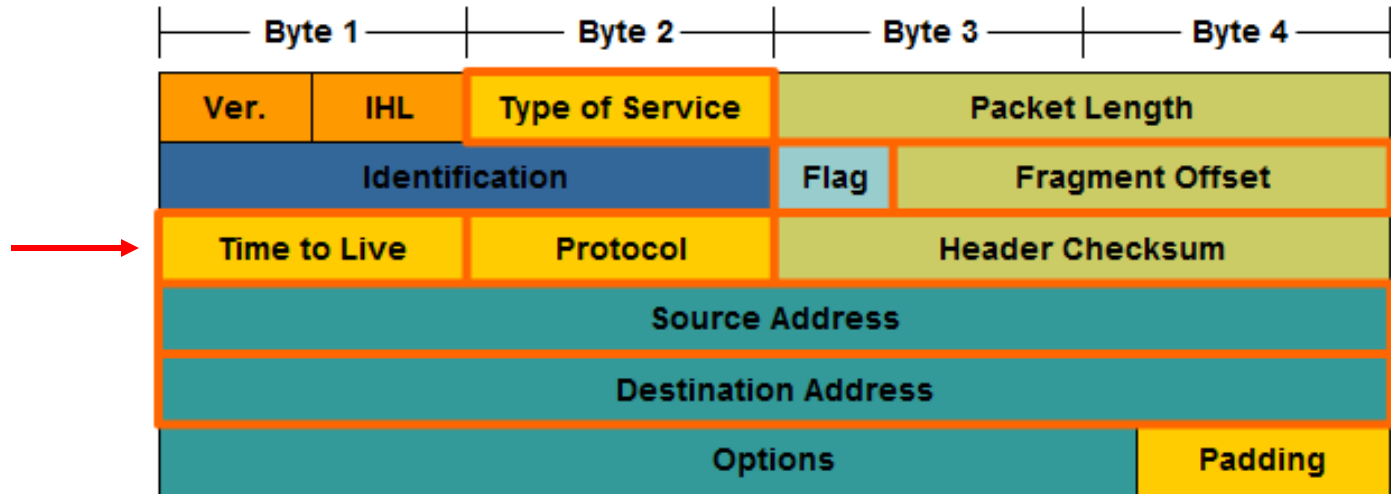
IP's TTL - Time To Live field



- If the router decrements the TTL field to 0, it will then drop the packet (unless the packet is destined specifically for the router, i.e. ping, telnet, etc.).
- Common operating system TTL values are:
 - UNIX: **255**
 - Linux: **64 or 255** depending upon vendor and version
 - Microsoft Windows 95: **32**
 - Other Microsoft Windows operating systems: **128**

IP's TTL - Time To Live field

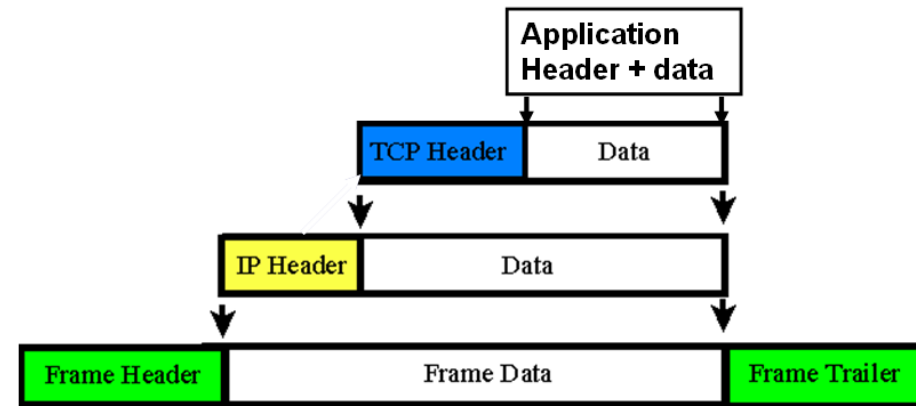
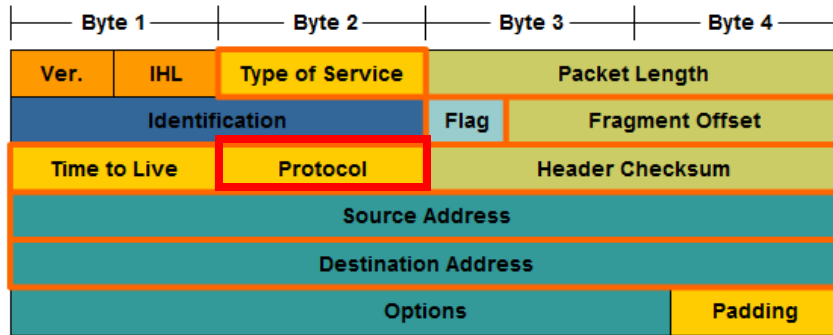
Decrement by 1, if 0
drop the packet.



- The idea behind the TTL field is that IP packets can not travel around the Internet forever, from router to router.
- Eventually, the packet's TTL which reach 0 and be dropped by the router, even if there is a routing loop somewhere in the network.

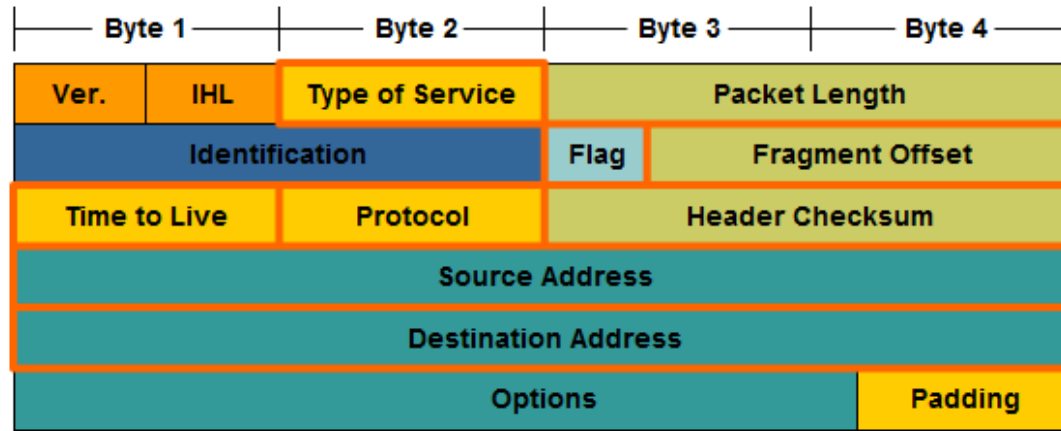
RS: TTL errors are used by traceroute and mtr to discover the path a packet takes

IP's Protocol Field



- **Protocol field** enables the Network layer to pass the data to the appropriate upper-layer protocol.
- Example values are:
 - 01 ICMP
 - 06 TCP
 - 17 UDP

Other IPv4 fields



- **Version** - Contains the IP version number (4)
- **Header Length (IHL)** - Specifies the size of the packet header.
- **Packet Length** - This field gives the entire packet size, including header and data, in bytes.
- **Identification** - This field is primarily used for uniquely identifying fragments of an original IP packet
- **Header Checksum** - The checksum field is used for error checking the packet header.
- **Options** - There is provision for additional fields in the IPv4 header to provide other services but these are rarely used.

Viewing Layer 3 information with Wireshark

No.	Time	Source	Destination	Protocol	Leng	Info
41	19.321087319	10.76.5.150	172.30.10.160	HTTP	68	GET / HTTP/1.0
42	19.322005417	172.30.10.160	10.76.5.150	TCP	66	80 → 54788 [ACK] Seq=1 Ack=19 Win=14592 Le...
43	19.322348239	172.30.10.160	10.76.5.150	HTTP	490	HTTP/1.1 200 OK (text/html)
44	19.322361391	10.76.5.150	172.30.10.160	TCP	66	54788 → 80 [ACK] Seq=19 Ack=425 win=30336 ...
45	19.322412549	172.30.10.160	10.76.5.150	TCP	66	80 → 54788 [FIN, ACK] Seq=425 Ack=19 Win=1...
46	19.322580304	10.76.5.150	172.30.10.160	TCP	66	54788 → 80 [FIN, ACK] Seq=19 Ack=426 Win=3...

▶ Frame 44: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0
 ▶ Ethernet II, Src: Vmware_af:e6:bd (00:50:56:af:e6:bd), Dst: Vmware_af:f2:c3 (00:50:56:af:f2:c3)
 ▼ **Internet Protocol Version 4, Src: 10.76.5.150, Dst: 172.30.10.160**

- 0100 = Version: 4
- 0101 = Header Length: 20 bytes (5)
- ▶ Differentiated Services Field: 0x10 (DSCP: Unknown, ECN: Not-ECT)
 - Total Length: 52
 - Identification: 0xff8b (65419)
- ▶ Flags: 0x02 (Don't Fragment)
 - Fragment offset: 0
 - Time to live: 64**
 - Protocol: TCP (6)**
- ▶ Header checksum: 0x7488 [validation disabled]
 - Source: 10.76.5.150**
 - Destination: 172.30.10.160**
 - [Source GeoIP: Unknown]
 - [Destination GeoIP: Unknown]

Time to Live (TTL)
Protocol of the data carried in the payload

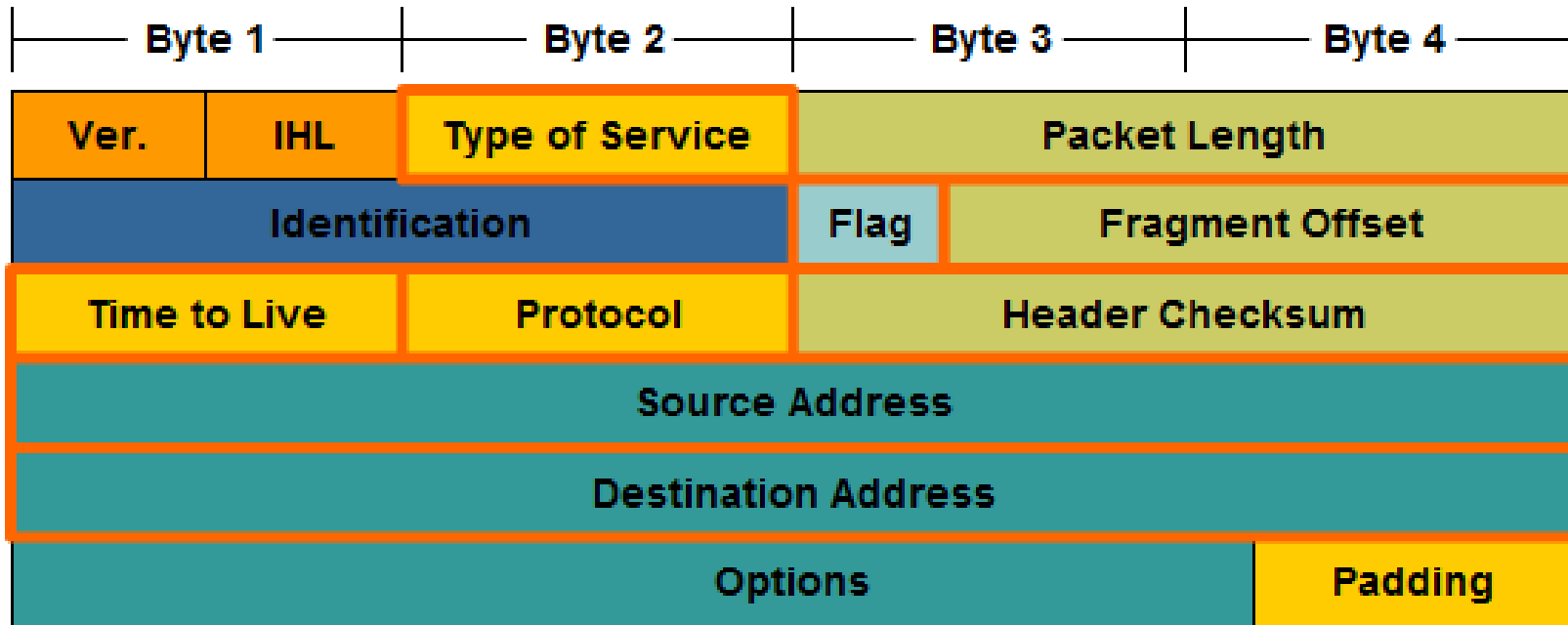
Source and destination IP addresses

▶ Transmission Control Protocol, Src Port: 54788 (54788), Dst Port: 80 (80), Seq: 19, Ack: 425, Len: 0

Traffic between EH-Centos VM and EH-Kali VM

IPv4 addressing & subnetting

IPv4 Addresses



- IPv4 addresses are 32 bit addresses

IPv4 Addresses

- IPv4 Addresses are 32 bit addresses:

1010100111000111010001011000100

10101001 11000111 01000101 10001001

- We use dotted notation (or dotted decimal notation) to represent the value of each byte (octet) of the IP address in decimal.

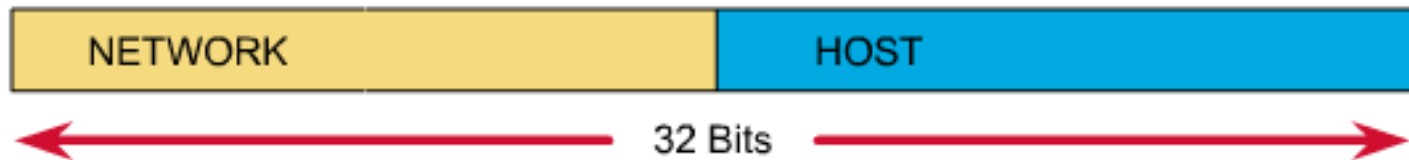
10101001 11000111 01000101 10001001

169 . 199 . 69 . 137

IPv4 Addresses

An IP address has two parts:

- **network number**
- **host number**



Which bits refer to the network number?

Which bits refer to the host number?

IPv4 Addresses

Answer:

- Newer technology - **Classless IP Addressing**
 - The **subnet mask** determines the network portion and the host portion.
 - Value of first octet does NOT matter (older classful IP addressing)
 - Hosts and Classless Inter-Domain Routing (**CIDR**).
 - Classless IP Addressing is what is used within the Internet and in most internal networks.
- Older technology - **Classful IP Addressing**
 - **Value of first octet** determines the network portion and the host portion.
 - Used with classful routing protocols like RIPv1.
 - The Cisco IP Routing Table is structured in a classful manner (CIS 82)

Network Addresses have all 0's in the host portion.

Network Address

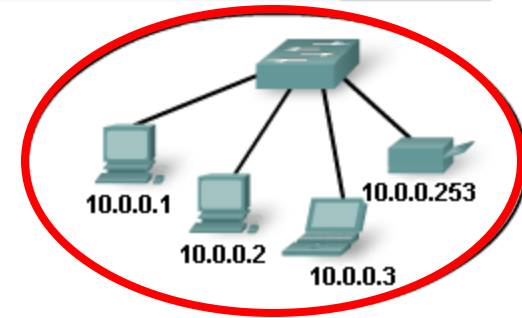
Broadcast Address

Host Address

Roll over to learn more.

Network			Host
10	0	0	0
00001010	00000000	00000000	00000000
10	0	0	255
00001010	00000000	00000000	11111111
10	0	0	1
00001010	00000000	00000000	00000001

Subnet Mask: 255.255.255.0



- **Network address** - The address by which we refer to the network
- **Broadcast address** - A special address used to send data to all hosts in the network
- **Host addresses** - The addresses assigned to the end devices in the network

Broadcast Addresses have all 1's in the host portion.

Network Address

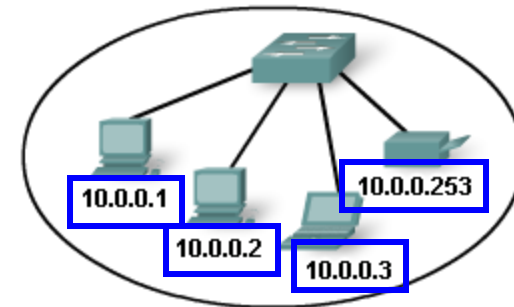
Broadcast Address

Host Address

Roll over to learn more.

Subnet Mask: 255.255.255.0

Network			Host
10	0	0	0
00001010	00000000	00000000	00000000
10	0	0	255
00001010	00000000	00000000	11111111
10	0	0	1
00001010	00000000	00000000	00000001



- **Network address** - The address by which we refer to the network
- **Broadcast address** - A special address used to send data to all hosts in the network
- **Host addresses** - The addresses assigned to the end devices in the network

Types of Addresses

Network Address

Broadcast Address

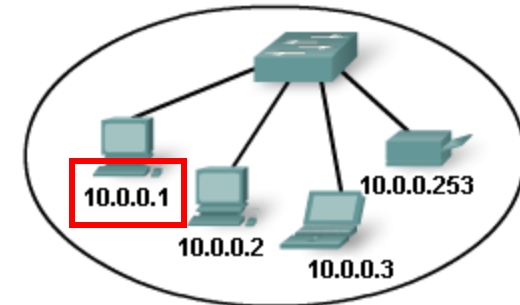
Host Address

Roll over to learn more.

Host Addresses can not have all 0's or all 1's in the host portion.

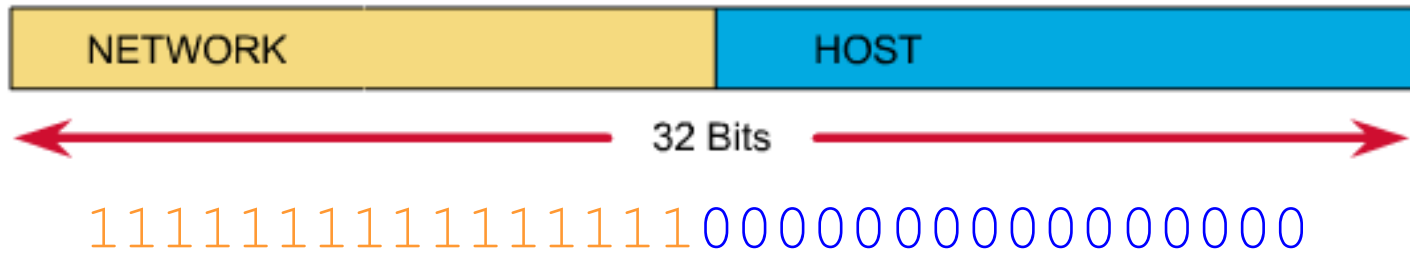
Subnet Mask: 255.255.255.0

Network			Host
10	0	0	0
00001010	00000000	00000000	00000000
10	0	0	255
00001010	00000000	00000000	11111111
10	0	0	1
00001010	00000000	00000000	00000001



- **Network address** - The address by which we refer to the network
- **Broadcast address** - A special address used to send data to all hosts in the network
- **Host addresses** - The addresses assigned to the end devices in the network

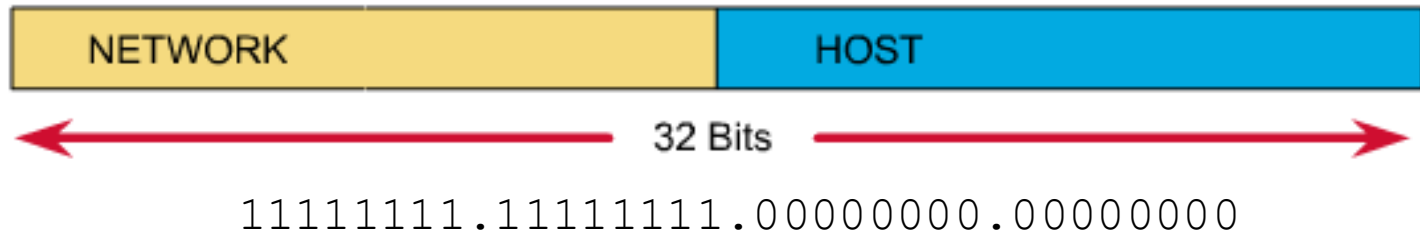
Dividing the Network and Host Portions



- **Subnet Mask**

- Used to define the:
 - Network portion
 - Host portion
- 32 bits
- Contiguous set of 1's followed by a contiguous set of 0's
 - 1's: Network portion
 - 0's: Host portion

Dividing the Network and Host Portions



Dotted decimal: 255 . 255 . 0 . 0

Slash notation: /16

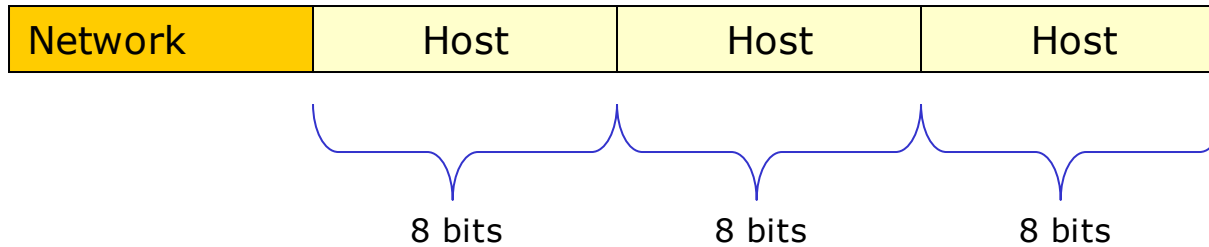
- Subnet mask expressed as:
 - Dotted decimal
 - Ex: 255.255.0.0
 - Slash notation or prefix length
 - /16 (the number of one bits)

Why the mask matters: Number of hosts!

Subnet Mask:	1st octet	2nd octet	3rd octet	4th octet
255.0.0.0 or /8	Network	Host	Host	Host
255.255.0.0 or /16	Network	Network	Host	Host
255.255.255.0 or /24	Network	Network	Network	Host

- The more host bits in the subnet mask means the more hosts in the network.
- Subnet masks do not have to end on "natural octet boundaries"

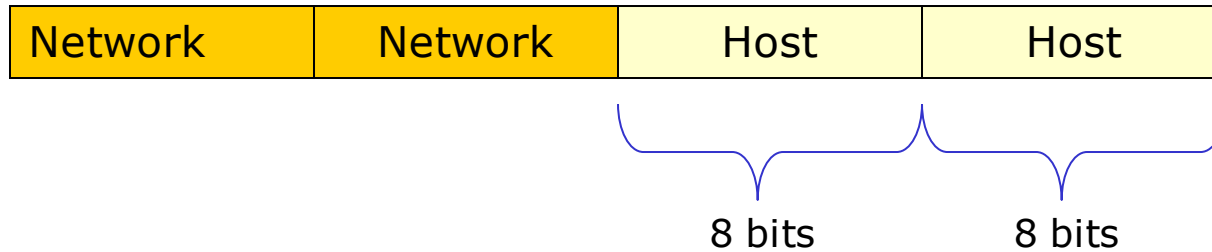
Subnet: 255.0.0.0 (/8)



With 24 bits available for hosts, there are 2^{24} possible addresses. That's 16,777,216 nodes!

- Only large organizations such as the military, government agencies, universities, and large corporations have networks with these many addresses.
- Example: A certain cable modem ISP has 24.0.0.0 and a DSL ISP has 63.0.0.0

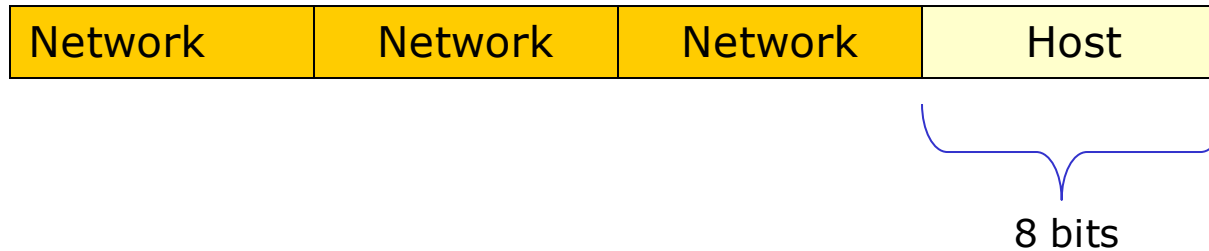
Subnet: 255.255.0.0 (/16)



With 16 bits available for hosts, there are 2^{16} possible addresses. That's 65,536 nodes!

- 65,534 host addresses, one for network address and one for broadcast address.

Subnet: 255.255.255.0 (/24)

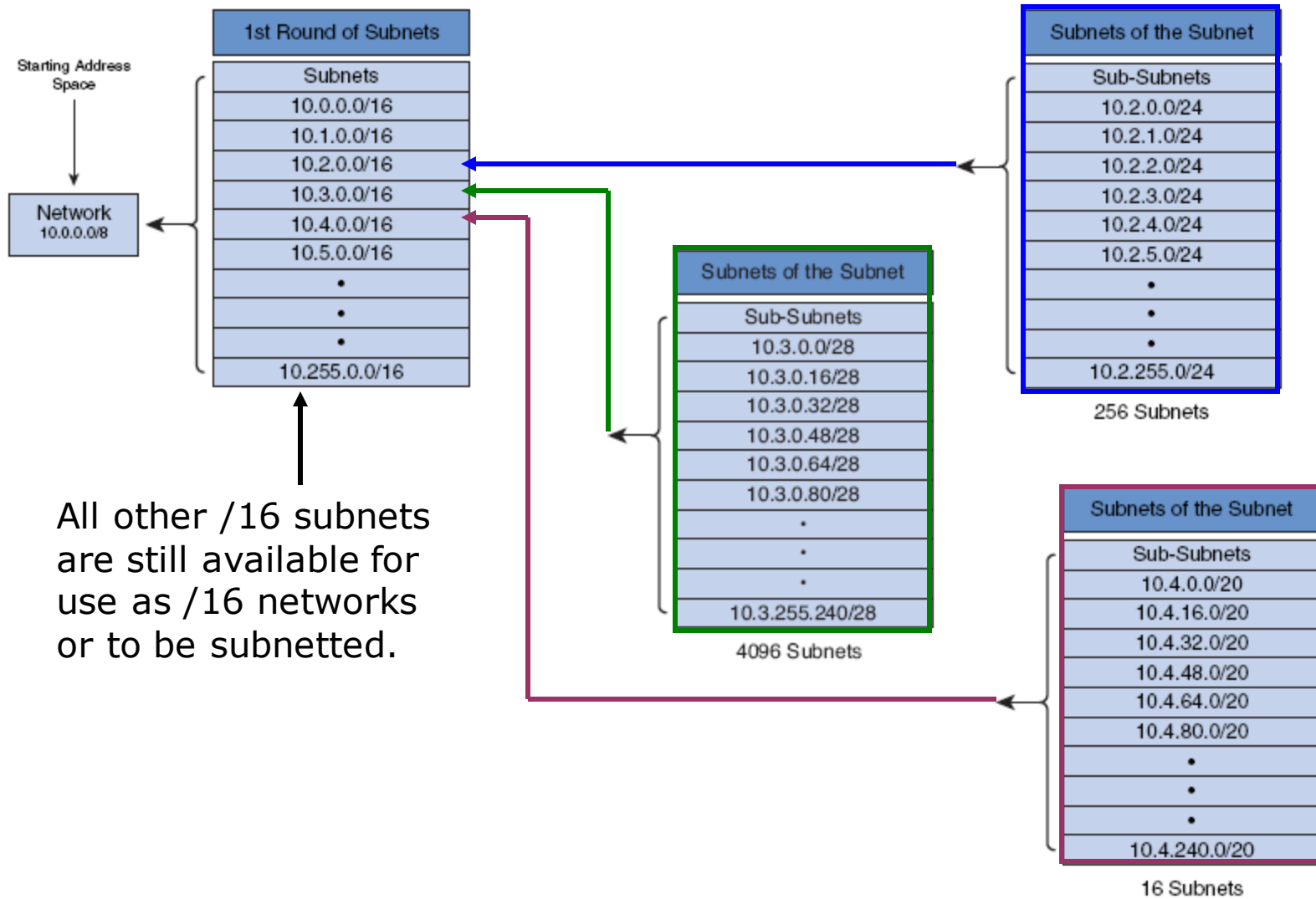


With 8 bits available for hosts, there are 2^8 possible addresses. That's 256 nodes!

- 254 host addresses, one for network address and one for broadcast address.

VLSM - Variable Length Subnet Masks

Subnet a subnet



Special Unicast IPv4 Addresses

- **Default Route**

Use the following IP address:

IP address:	192 . 168 . 1 . 100
Subnet mask:	255 . 255 . 255 . 0
Default gateway:	192 . 168 . 1 . 1

- **Loopback Address**

- Special address that hosts use to direct traffic to themselves.
- 127.0.0.0 to 127.255.255.255

- **Link-Local Addresses (APIPA)**

- 169.254.0.0 to 169.254.255.255 (169.254.0.0 /16)
- Can be automatically assigned to the local host by the operating system in environments where no IP configuration is available.
- Microsoft calls this APIPA (Automatic Private IP Addressing)

- **TEST-NET Addresses**

- 192.0.2.0 to 192.0.2.255 (192.0.2.0 /24)
- Set aside for teaching and learning purposes.
- These addresses can be used in documentation and network examples.

Rick Graziani
Cabrillo College



1.2 Introducing IPv6

Introducing IPv6

- Not a “new” protocol.
- Developed mid to late 1990s.
- Much learned from IPv4.
- 128-bit address space, written in hexadecimal.
- This gives us 340 undecillion addresses!



128 bits

128 bits



2001:DB8:CAFE:0001::100

340 undecillion

= 340,282,366,920,938,463,463,374,607,431,768,211,456

IPv6

- How many is 340 undecillion?
- 340 undecillion addresses is 10 nonillion addresses per person!
- Internet is a much different place and will continue to evolve:
 - Mobile devices
 - Video on demand
 - Internet of Everything
 - A critical part in how we “live, work, play, and learn”.



10 nonillion

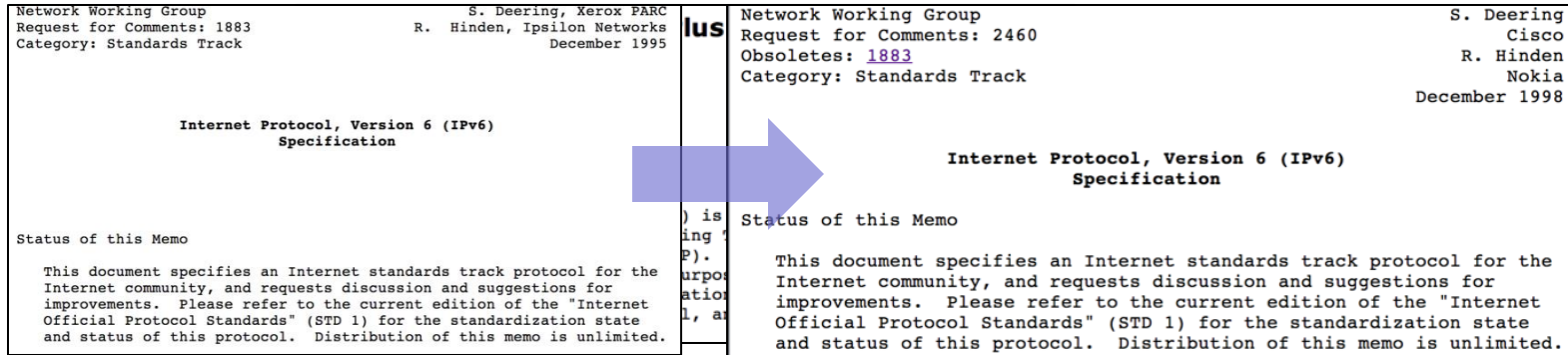
= 10,000,000,000,000,000,000,000,000,000,000

IPv6

- IPv6 is not just about more addresses:
 - Stateless autoconfiguration
 - End-to-end reachability without private addresses and NAT
 - Better support for mobility
 - Peer-to-peer networking easier to create and maintain, and services such as VoIP and Quality of Service (QoS) become more robust.

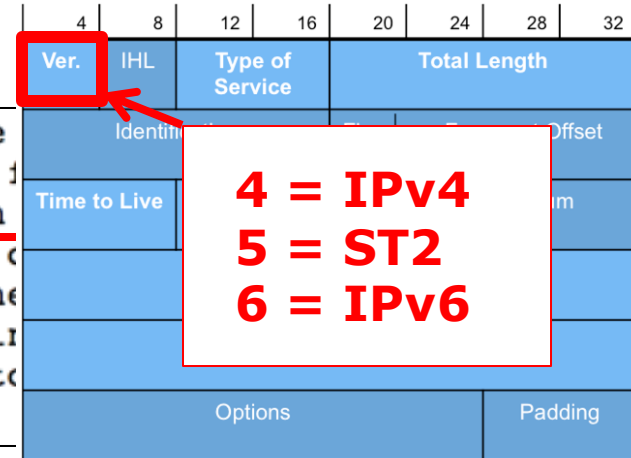


IPv6: A Brief History



- 1993, IETF announced a call for white papers with RFC 1550 *IP: Next Generation (IPng) White Paper Solicitation*.
- IETF chose Simple Internet Protocol Plus (SIPP) written by Steve Deering, Paul Francis, and Bob Hinden but changed the address size from 64 bits to 128 bits.
- 1995, IETF published RFC 1883 Internet Protocol, Version 6 (IPv6) Specification - later obsoleted by RFC 2460 in 1998.

What About IPv5?

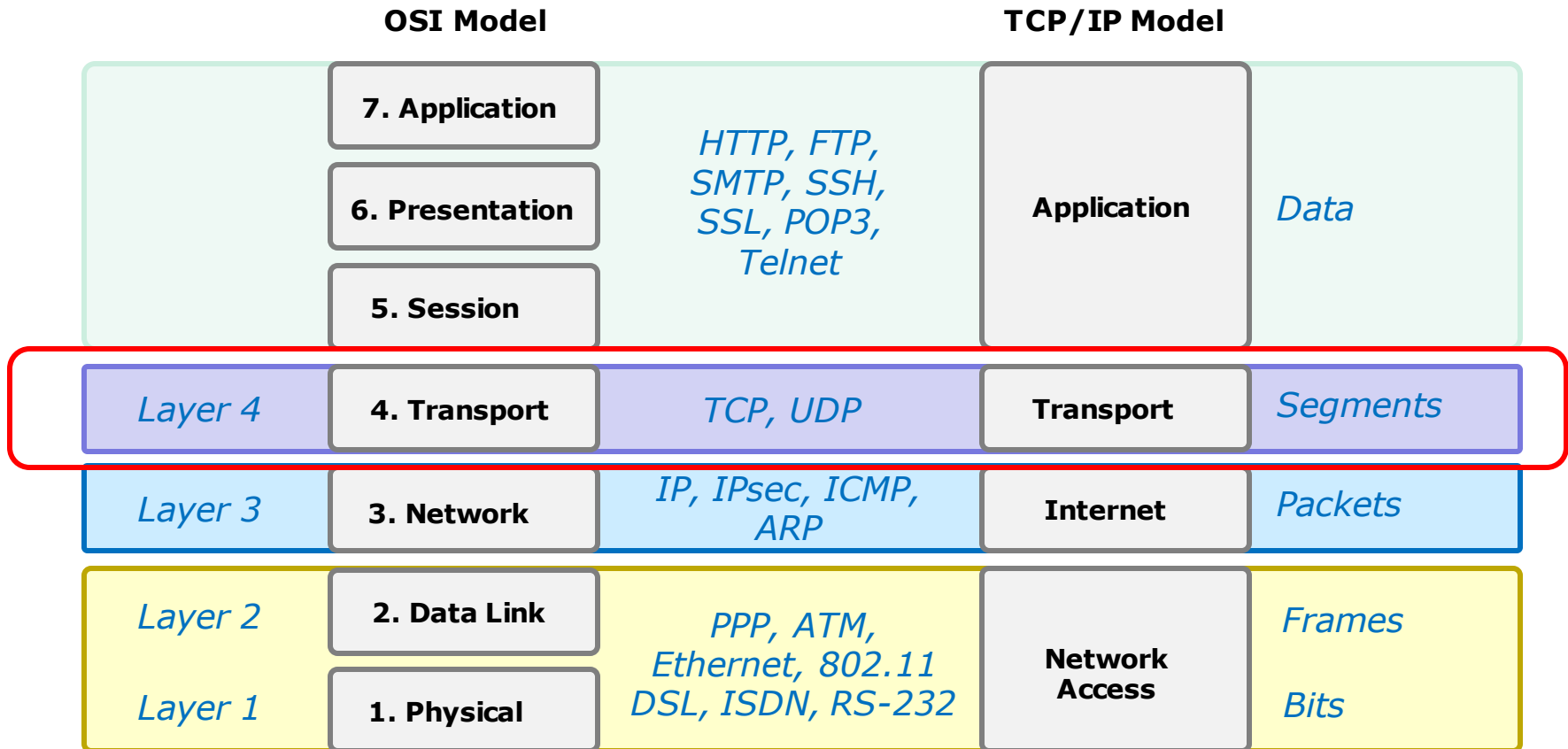


The ST packet header is not constrained to be compatible with the IP packet header, except for the IP Version Number (the 4 bits) that is used to distinguish ST packets (IP Version 5) from IP packets (IP Version 4). The ST packets, or protocol data units (PDUs), can be encapsulated in IP either to provide connectivity (possibly with degraded service) across portions of an internetwork that do not provide support for ST, or to allow access to services such as security that are not provided directly by ST.

- In the late 1970s, a family of experimental protocols was developed intended to provide quality of service (QoS) for real-time multimedia applications such as video and voice.
- Known as Internet Stream Protocol (ST) and later ST2 – (RFC 1190 and RFC 1819).
- Although it was never known as IPv5, when encapsulated in IP, ST uses IP Protocol version 5.

Transport Layer

OSI and TCP/IP Models



*Open Systems
Interconnection model*

*Model used to
build the Internet*

Transport Layer

The Protocols

There are two primary protocols operating at the Transport layer:

User Datagram Protocol (UDP)

Connectionless (*snmp traps are "fire and forget"*)

Stateless

Unreliable

The UDP packet is called a **packet**

Transmission Control Protocol (TCP)

Connection-oriented

Stateful (*like new or established states in firewalls*)

Reliable The TCP packet is called a **segment**



TCP Header

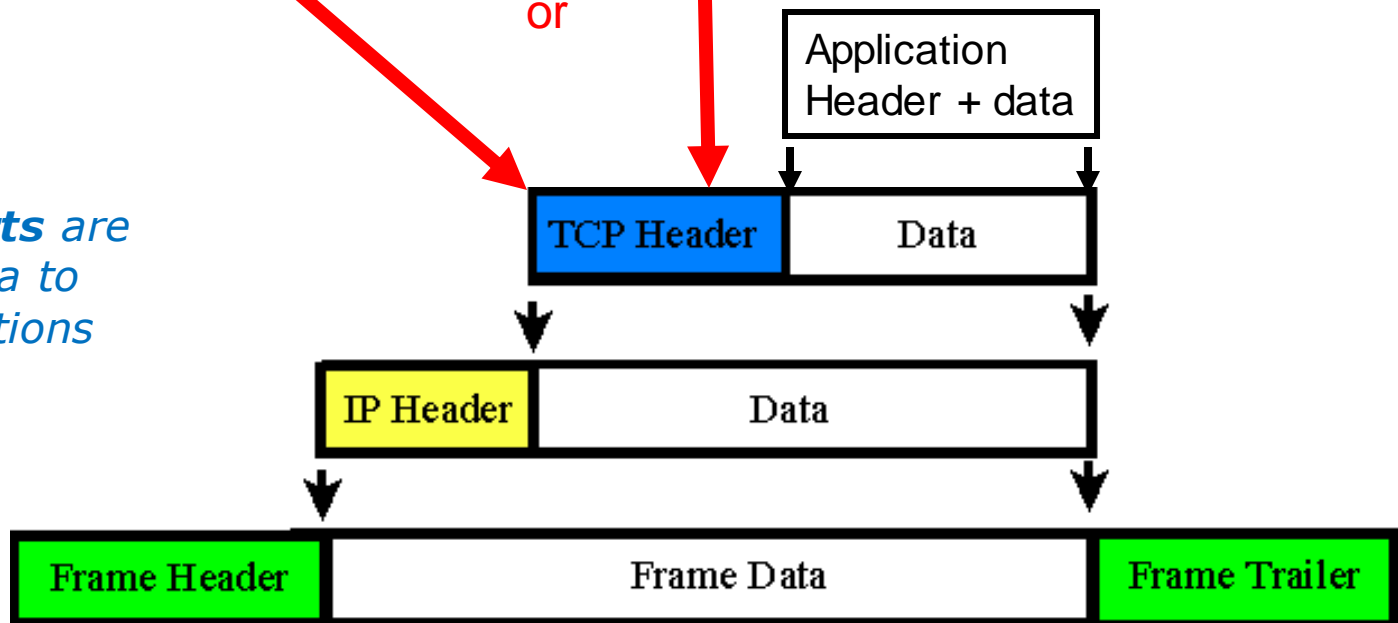
Source Port (16 bits)		Destination Port (16 bits)						
Sequence Number (32 bits)								
Acknowledgement Number (32 bits)								
Data Offset (4 bits)	Reserved (6 bits)	URG	ACK	PSH	RST	SYN	FIN	Window (16 bits)
Checksum (16 bits)		Urgent Pointer (16 bits)						
Options and Padding								

UDP Header

Source Port (16 bits)		Destination Port (16 bits)	
Length (16 bits)		Checksum (16 bits)	
Data....			

or

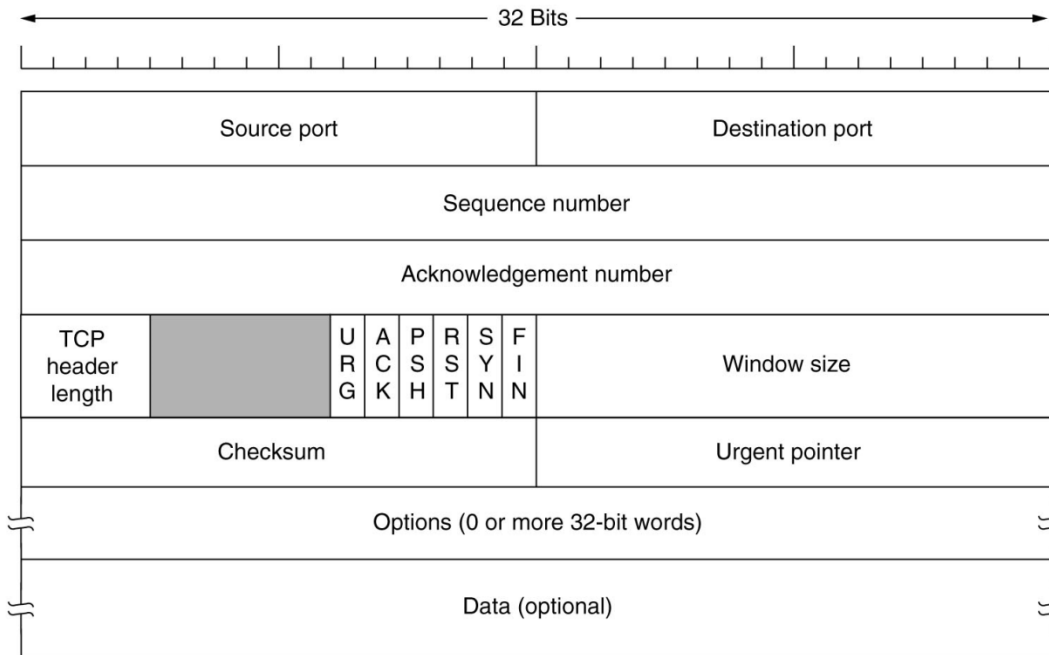
*The source and destination **ports** are used to get data to specific applications*



Transport Layer

The Transmission Control Protocol

TCP Header



*The source and destination addresses at this level are **ports***

Sequence and acknowledgement numbers are used for flow control.

ACK, SYN and FIN flags are used for initiating connections, acknowledging data received and terminating connections

Window size is used to communicate buffer size of recipient.

Options like SACK permit selective acknowledgement

Transport Layer



Host A

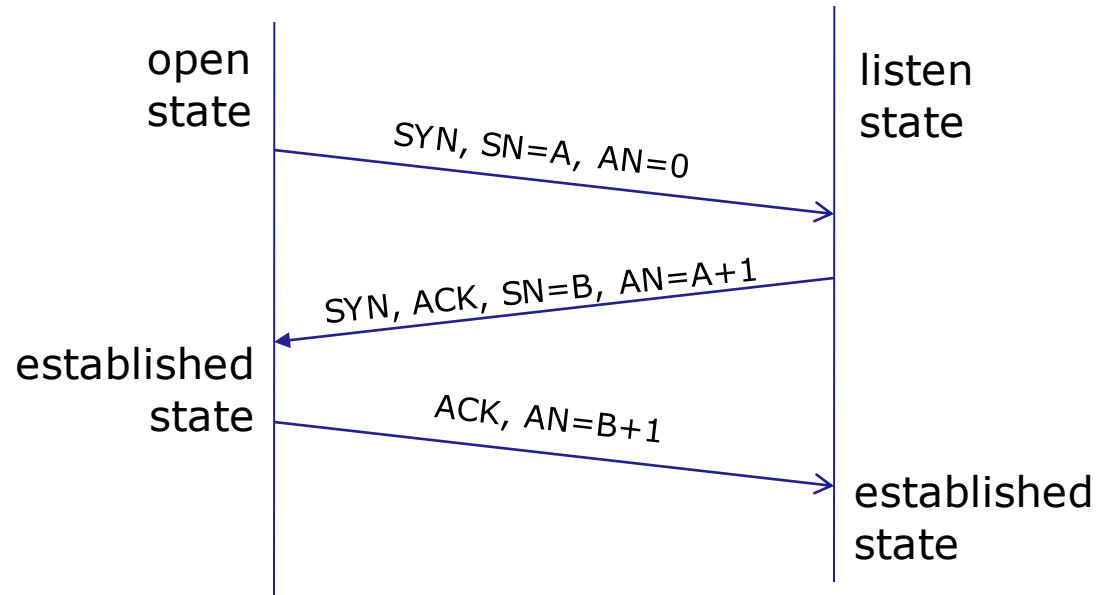


Host B

3-Way Handshake

Initiating a new TCP Connection

1. SYN
2. SYN-ACK
3. ACK



AN=Acknowledgment Number
SN=Sequence Number
ACK=ACK flag set
SYN=SYN flag set

Transport Layer

Sockets

Sockets are communication endpoints which define a network connection between two computers (RFC 793).

- Source IP address
- Source port number
- Destination IP address
- Destination port number



The socket is associated with a port number so that the TCP layer can identify the application to send data to.

Application programs can read and write to a socket just like they do with files.

Transport Layer

The Transmission Control Protocol (TCP)

Continuing communications on an established connection

- o The Sliding Window

Used for flow control - allows sending additional segments before an acknowledgement is received based on recipients buffer size

- o Flow Control (cumulative acknowledgment)

Recipient tells sender the size of its input buffer and sends acknowledgements (ACKs) when data has been received. Sequence numbers are used to detect missing segments.

- o The SACK option

Selective acknowledgement so only the dropped segments need to be retransmitted.

- o The RST Flag

Used to terminate a connection when an abnormal situation happens

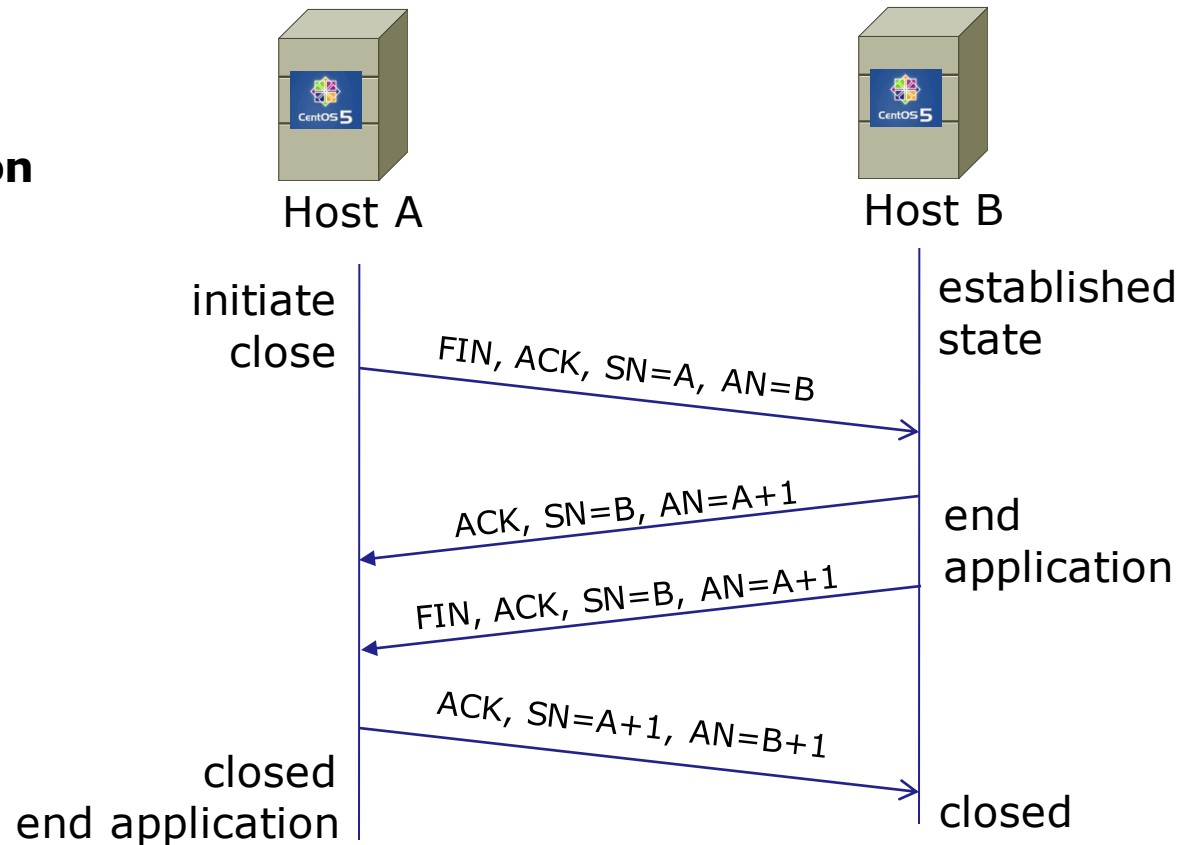
Transport Layer

Closing a TCP Connection

Four-Way Handshake

1. FIN, ACK
2. ACK
3. FIN, ACK
4. ACK

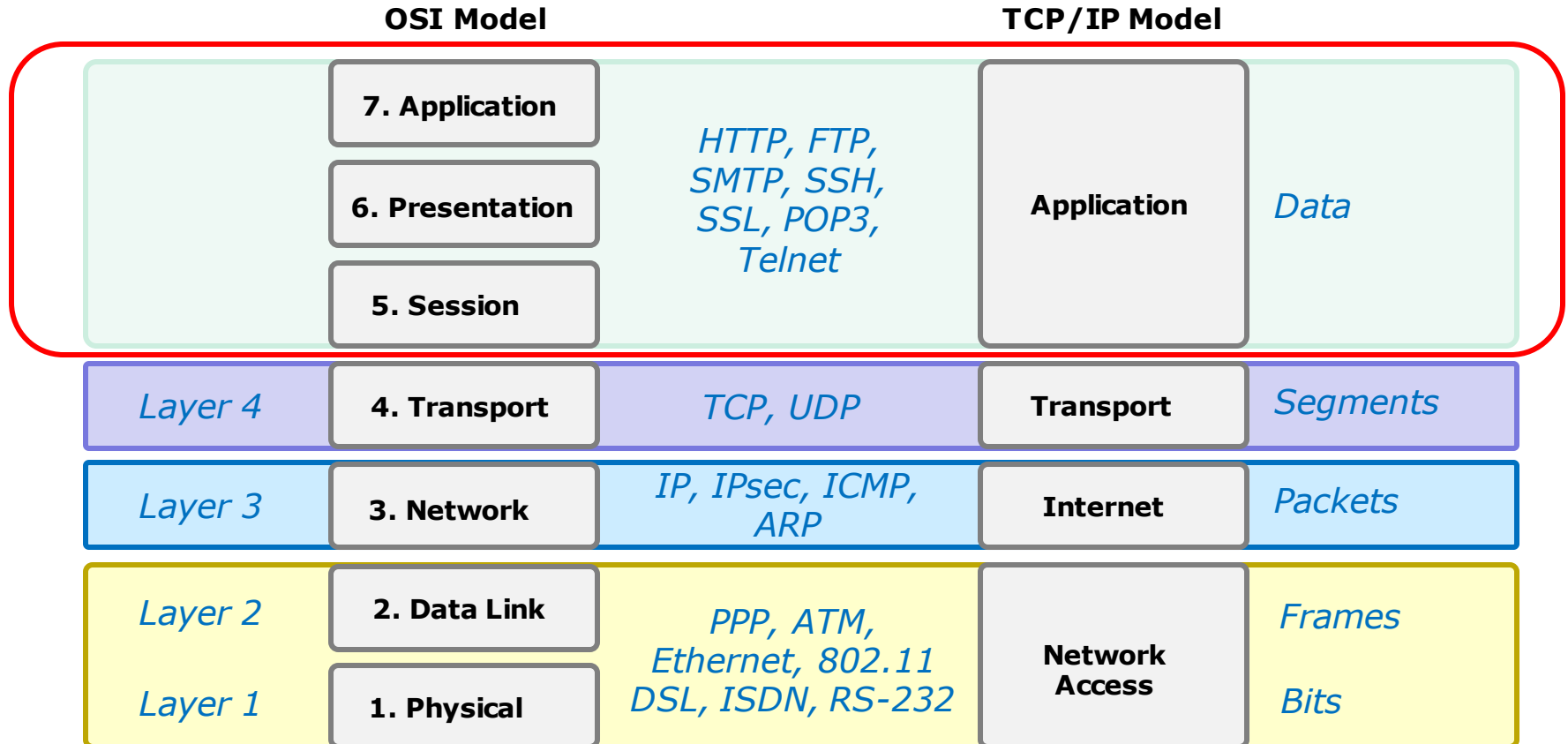
Closing with a shorter three-way handshake is also possible, where the Host A sends a FIN and Host B replies with a FIN & ACK (combining two steps into one) and Host A replies with an ACK.



AN=Acknowledgment Number
 SN=Sequence Number
 ACK=ACK flag set
 FIN=FIN flag set

Application Layer

OSI and TCP/IP Models



*Open Systems
Interconnection model*

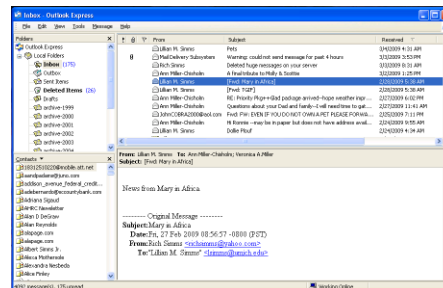
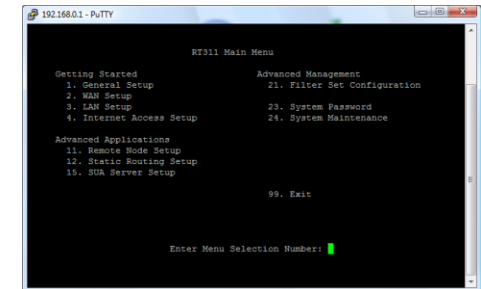
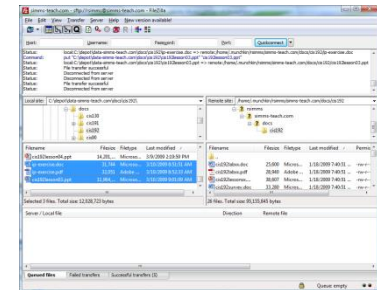
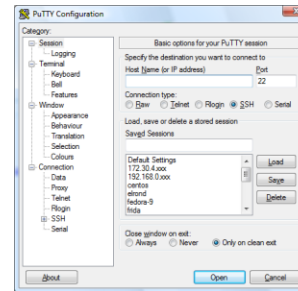
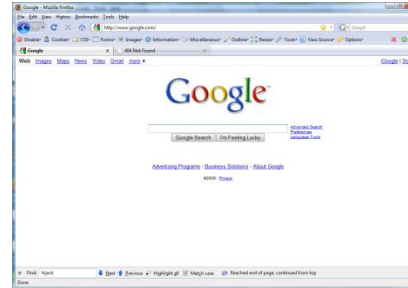
*Model used to
build the Internet*

Application Layer

Applications

Examples:

- Web servers
- FTP servers
- SSH daemon
- Telnet server
- Mail servers



Application Layer

Responsibilities of Applications

Network connections, routing, and transfer of data are all taken care of by the lower layers of the protocol stack. What must applications do?

- Authenticate users
- Control access
- Log important information
- Format data (compress/encrypt)
- Provide whatever functionality is desired.

Application Layer

The Client-Server Model

Clients

Programs that are generally run on demand, and initiate the network connection to the server.

Examples: telnet, ftp, ssh, browsers, email clients.

Servers

Programs (services/daemons) that are constantly running in the background waiting for client connections.

- Services and Ports: */etc/services*
- Architecture:
 - Direct or iterative servers – listen to a particular port and directly responds to requests
 - Indirect or concurrent servers (e.g. super daemons) – listen to a particular port and then starts up another server program to process the request

Service Ports

Last week we talked about Layer 4 ports. Ports are used to direct requests to the appropriate service/application

< snipped >

21 is registered to ftp, but also used by fsp

```
ftp          21/tcp
ftp          21/udp          fsp fspd
ssh         22/tcp          # SSH Remote Login Protocol
ssh         22/udp          # SSH Remote Login Protocol
telnet     23/tcp
telnet     23/udp
```

24 - private mail system

```
lmtpl      24/tcp          # LMTP Mail Delivery
lmtpl      24/udp          # LMTP Mail Delivery
smtp       25/tcp          mail
smtp       25/udp          mail
```

< snipped >

```
domain     53/tcp          # name-domain server
domain     53/udp
whois++    63/tcp
whois++    63/udp
bootps     67/tcp          # BOOTP server
bootps     67/udp
bootpc     68/tcp          dhcpc        # BOOTP client
bootpc     68/udp          dhcpc
tftp       69/tcp
tftp       69/udp
finger     79/tcp
finger     79/udp
http       80/tcp          www www-http # WorldWideWeb HTTP
http       80/udp          www www-http # HyperText Transfer Protocol
kerberos   88/tcp          kerberos5 krb5 # Kerberos v5
```

< snipped >

Assignment



Rich's Cabrillo College CIS Classes
CIS 76 Calendar

Home Resources Forums CIS Lab Canvas

Login
Flashcards
Admin

CIS 76
CIS 90
Previous Terms

102 days till term ends!

Cabrillo College
Web Advisor
Commands and Files

VLab (classic)
VLab (web)
NETLAB+

CIS 76 VLab Pod Assignments

CIS 90 VLab VM Assignments

RIP Dennis Ritchie

CIS 76 (Fall 2016)
Course Home Grad

Topics covered below

Lesson	Date
1	8/30

Netlab+ link on left panel

BACCC
BAY AREA
COMMUNITY COLLEGE CONSORTIUM

NETLAB+

BACCC NETLAB Security System 2

Username:

Password:

Login

[Forgot Password?](#)

POWERED BY
NDG
NETLAB+

NETLAB+® provides remote access to lab equipment and curriculum. To access, you need a user ID and password, assigned by your instructor or local system administrator.

Personal firewall software can interfere with this application. If you experience login or port test failures, please disable your firewall software to determine if this is causing the problem.

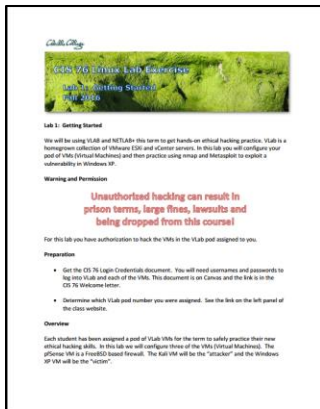
Browser security settings can interfere with required features. It is recommended that you add the IP address (or host name) of this site to your browser's trusted site list. This application uses **Java™**, JavaScript, Cookies, Popup Windows, and IFRAMES. Please adjust your browser settings accordingly.

System Web Browser Version Status

Lab Assignments

Pearls of Wisdom:

- Don't wait till the last minute to start.
- The *slower* you go the *sooner* you will be finished.
- A few minutes reading the forum can save you hour(s).
- Line up materials, references, equipment, and software ahead of time.
- It's best if you fully understand each step as you do it. Refer back to lesson slides to understand the commands you are using.
- Use Google for trouble-shooting and looking up supplemental info.
- Keep a growing cheat sheet of commands and examples.
- Study groups are very productive and beneficial.
- Use the forum to collaborate, ask questions, get clarifications, and share tips you learned while doing a lab.
- Plan for things to go wrong and give yourself time to ask questions and get answers.
- **Late work is not accepted** so submit what you have for partial credit.





Wrap up

Next Class

Assignment: Check the Calendar Page on the web site to see what is due next week.

Lab 2

Quiz questions for next class:

- What standard port is used for HTTP?
- How many bits make up an IPv6 address?
- True or false: UDP is a connectionless protocol?



Backup