University of Washington

INFO 341 - Computer Networks and Distributed Applications

Fall Quarter, 2016

Course Objectives

In this course, students will learn to apply technical principles of networks and distributed applications towards developing robust architectures of computing, network infrastructure and systems. By the end of the course, students will demonstrate analysis and evaluation skills in the evaluation, selection and implementation of different network carriers infrastructure, technologies, Internet Service Providers (ISPs), Internet-based applications, as well as comparing the attributes of network/transmission media (copper, fiber, RF/wireless).

In this course, students will learn to apply technical principles of networks and distributed applications towards developing robust architectures of computing, network infrastructure and systems. By the end of the course, students will demonstrate analysis and evaluation skills in the evaluation, selection and implementation of different network carriers infrastructure, technologies, Internet Service Providers (ISPs), Internet-based applications, as well as comparing the attributes of network/transmission media (copper, fiber, RF/wireless).

Through use cases, case studies and labs, students will demonstrate understanding of computer network technologies including standard terminology, communications interfaces and protocols including;

- Local Area Networks, Ethernet and MAC Layer protocols
- TCP/IP protocol suite and TCP/IP based applications
- LAN interconnection; LAN Switching, IP routing and routing protocols
- IEEE 802.11 Wireless LANs and Wireless technologies including RFID
- IP based network services
- Network management tools
- Network security considerations

Achieve a working understanding of networking protocols by studying and applying class theory and concepts to lab environments and real world use cases/case studies.

Apply knowledge of the OSI model/reference architecture to network and CyberSecurity mechanisms utilized in today's Internet environment including protocol analyzers, network routers/access control lists and packet filters.

Demonstrate knowledge of distributed applications including:

- Evaluating data center design alternatives
- Analyzing distributed application environments in network/Internet based environments
- Assess application high availability, fail-over strategies and business continuity
- Apply knowledge of network protocols and infrastructure to application latency, performance analysis and mitigation

- Demonstrate understanding of technical and operational constraints by assessing risk and business implications of geographically distributed applications and global infrastructure environments
- Demonstrate understanding of cloud computing and virtual infrastructure environments to use case/case study environments evaluating the technical and business feasibility from a network and cyber security perspective.

Apply network and distributed application concepts in UW Informatics Information Assurance and Cybersecurity coursework.

Develop related skills to succeed in applying network and distributed application concepts to business environments

Course Administration

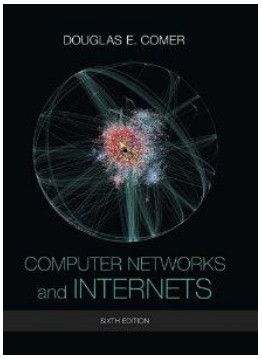
Attendance

Students are expected to attend all classes unless a sufficient excuse is provided or prior arrangements are made with the instructor.

Textbook (RECOMMENDED – Not Required)

Computer Networks and Internets, Douglas Comer

ISBN-10: 013358793-2 Publisher: Pearson, 2014
ISBN-13: 978013358793-7



Participation

As stated in the syllabus, class participation is important. Please read the assignments ***before*** class. Discussions will focus on that week's topics.

Assignments & Late Policy

There will be a 10% late penalty per day for late assignments. Assignments over a week late not accepted, unless absence approved in advance.

Scholastic Honesty

Scholastic dishonesty is broadly any act which violates the rights of other students in the execution and evaluation of their work, or which involves misrepresentations of the work of another as one's own. You are expected to do your own work. In addition, all students will be expected to sign and date the policy statement at the end of the syllabus.

Also students are expected to adhere to the highest standards of ethical behavior and sign the computer lab use policy at the end of the syllabus the first week of class.

Grading

Participation (current events, class discussion, reading)	5%
Quizzes	20%
Midterm Exam	25%
Labs (lab deliverables, lab execution)	20%
Final Exam	30%
	100%

Course Progression

The following is the class progression covering the 10 weeks for the course. The class will meet three times a week, twice in lecture for 1 hour and 50 minutes and once in lab for 50 minutes. Every class will start with a 10 minute review of current events. This will familiarize students with the network and network-enabled happenings in the world and provide real world to anchor what they will be learning in lecture.

Week 1: Overview

HW Handouts, Comer Chapters 1-2, (L1 & L2)
L1 Syllabus, Course Overview, Types Nets Regulatory/Divestiture/Internet
L2 Protocols & Arch, OSI Model, TCP/IP, Internet trends
Lab LANs, Internet Resources

Week 2: Internet Applications

HW Handouts, Comer Chpts 3 (L1), Chapters 4 (L2),
L1 Internet Apps, Net Programming client-server, peer2peer, sockets
L2 Application Layer Protocols HTTP, SMTP, FTP, DNS
Lab Network Frame Capture

Week 3: Data Communications,

HW Handouts, Comer Chapters 5,6,7 (L1), Chapter 8 (L2)
L1 Data Comm, Overview, Signaling, Media
L2 Transmission Media, Chan Coding (CRC),
Lab Data Link protocol analysis

Week 4: Data Link Protocols and LANs

HW Handout, Comer Chapter 9, (L1), handout Chpts 13,14,15, (L2)
L1 Multiplexing, Data Link protocols
L2 LANs, MAC Layer protocols
Lab IP Addressing, Subnetting, routing

Week 5: Internet Protocol

HW Comer Chapters 20,21, Handout (L1) Comer Chapter 23,24,25, Handout (L2)
L1 TCP/IP protocol & layering
L2 IP Subnets/Subnet Masks
L2 ***Midterm Review***
Lab TCP/IP routed network

Week 6: Internet Protocol Routing

HW Comer Chapter 17, 26, Handout (L2)
L1 **MIDTERM EXAM**,
L2 IP Routing, LAN Interconnect
Lab TCP/IP routing protocols

Week 7: Application QoS/Perfomance

HW	Routing Protocols Handout (L1)
	Comer Chapter 27, Handout (L2)
L1	Routing Protocols
L2	Quality of Service (QoS)
Lab	Application Net Performance/Anal

Week 8 Internet Advanced Applications

HW	Comer Chapter 29, 30, Handout (L1)
	Comer Chapter 28, Handout (L2)
L1	Network Security, SNMP
L2	Voice over IP (VoIP)
Lab	Intro Net Security/ACL's

Week 9: Wireless/Mobility

HW	Read Comer Chapter 16, Handouts (L1, L2)
L1	RF Spectrum (licensed/unlicensed ISM)
	Intro Wireless LANs
L2	Wireless Arch, Design, RFID
Lab	Wireless Networking
	Wireless Net Design/Security/Monitor

Week 10: Network Tech Trends/Futures

HW	Comer Chpts 29-30, Handout (L1)
	Comer Chpts 32, 33, Handout (L2)
L1	Embedded Systems, SAAS
	Final Review.
L2	**i341 Final Examination**
Lab	No Lab (Final)

Week 1 – Overview

HW Read Comer Chapters 1-2, Handouts (L1 & L2)
L1 Syllabus, Course Overview, Types of Networks, Regulatory Environment, Divestiture, Internet Services model and business implications
L2 Network Architecture and Protocols, OSI Reference Model, TCP/IP, Internet based applications
Lab LANs, Networks, Internet Resources

Learning Objectives

Theory – After L1 and L2, students should be able to:

1. Understand the goals of the course
2. Describe the progression of the course and milestones
3. Comprehend the responsibilities of a network professional
4. Explain the proper computer lab use policy
5. Demonstrate that they understand the grading, attendance, participation and late day policies
6. Explain the key deliverables for the course
7. Assess types of network environments and Internet model
8. Apply the OSI reference model and relevance to computer networks and distributed applications
9. Demonstrate the importance of the TCP/IP (Internet based) protocols and architectures in lab and case studies

Lab and Practice – After completing this lab, students should be able to:

1. Develop understanding of LAN technologies, utilization
2. Identify credible sources of knowledge for network architectures and distributed applications.
3. Keep up to date on developments in the fields of communications, networks, and Internet based technologies.
4. Demonstrate the ability to be able to find various networking technology resources

Week 2 – Internet Applications

HW Comer Chapters 3-4 (L1), Handouts,
L1 Internet applications, network client-server, peer to peer, sockets
L2 Application Layer protocols (HTTP, SMTP, FTP, DNS)
Lab Network Frame File Capture, Internet Applications Lab

Learning Objectives

Theory – After L1 and L2, students should be able to:

1. Evaluate and compare design and integration drivers for supporting distributed applications in data center and cloud/virtual environments
2. Demonstrate ability to classify and describe TCP/IP applications SMTP, POP, IMAP for email, HTTP, Telnet and SSH, FTP, FTPS, & SFTP (file transfer), XMPP – their basic use and dependencies.
3. Assess application turns and relation to performance
4. Evaluate connection oriented transport protocol mechanisms
5. Explain TCP congestion control operation
6. Understand retransmission timers and window management
7. Apply the contributing elements and effects of latency to application analysis labs and case studies.
8. Distinguish impact of bandwidth versus latency on distributed application performance

Lab and Practice – After completing this lab, students should be able to:

1. Be able to capture Application ethernet frames off a live network
2. Explain the concept of protocol layering
3. Articulate the importance “chatty” protocols relevant to distributed application, client and systems performance
4. Identify key fields in an Ethernet frame
5. Describe how capturing Ethernet frames can be a valuable tool in analyzing and debugging connectivity and performance problems in distributed applications.
6. Apply understanding of the significance of application and data link frame captures to cyber security/network security.

Week 3 – Data Comm, Data Link Protocols

HW Comer Chapters 5,6,7, Handout (L1), Comer Chapter 8, Handout (L2)
L1 Transmission Media, Channel Coding (CRC),Data Communications overview
L2 Data Link Protocols,
Lab Data Link Protocols (DL frames, error correction//CRC)

Learning Objectives

Theory – After L1 and L2, students should be able to:

1. Demonstrate understanding of the issues involved in the evaluation, selection and implementation of different network media.
2. Analyze different carrier/telco provider services, and the cost and distributed application performance/reliability implications of different media offered as part of network infrastructure offerings.
3. Understand standard terminology and communications interfaces
4. Explain the key characteristics of data transmission
5. Distinguish advantages/disadvantages of different transmission media
6. Apply understanding of transmission media and data communications to case studies investigating distributed applications performance dependencies.
7. Describe/compare mechanisms for data link error checking

Lab and Practice – After completing this lab, students should be able to:

1. Apply understanding of transmission media on distributed/Internet application performance and reliability
2. Describe protocol framing, fields and error checking mechanisms (CRC).
3. Understand and describe the significance of transmission media related to cyber security threat monitoring, and protection mechanisms

Week 4 – Data Link Protocols and LANs

HW Comer Chapter 9, Handout (L1)
Comer Chapters 13,14,15 Handout (L2)
L1 Data Link Protocols, Multiplexing, LANs, MAC layer protocols
L2 Intro TCP/IP protocol stack
Lab TCP/IP addressing and subnetting/subnet masking

Learning Objectives

Theory – After L1 and L2, students should be able to:

1. Describe Local Area Network (LAN) technologies and standards
2. Identify advantages/disadvantages of different LAN topologies
3. Demonstrate an understanding of LAN contention/access methods and their impact from a business and operational perspective
4. Describe Ethernet technology, operation and frame format
5. Understand and describe the business and security implications of Ethernet in home, office LANs and Internet based environments
6. Describe common Ethernet design and operational mistakes
7. Demonstrate an understanding of TCP/IP protocol suite
8. Explain significance of private& public TCP/IP address spaces
9. Distinguish IPv4 Class A, Class B and Class C Networks
10. Demonstrate an understanding of TCP/IP subnetting & subnet masking
11. Describe TCP/IP protocol layering
12. Explain TCP and UDP differences in distributed applications
13. Explain the options to obtain TCP/IP addresses and business implications
14. Understand and describe the business and security implications of TCP/IP in business, research and Internet based environments

Lab and Practice – After completing this lab, students should be able to:

4. Demonstrate understanding LAN access methods, Ethernet contention and impact on distributed applications
5. Describe important Ethernet and TCP/IP protocol framing/fields
6. Demonstrate understanding TCP/IP subnet masking and TCP/IP address architectures in LAN & server farm/data center environments.
7. Demonstrate use of TCP/IP protocol in routed networks & Internet.
8. Understand and describe the significance of TCP/IP protocol layers in modern cyber security monitoring, firewall, packet filter, intrusion detection and protection mechanisms

Week 5 – IP Routing, Routing Protocols, ISP Peering

HW Comer Chapter 19, Handout (L1)
Routing Protocols Handout (L1-L2)
L1 IP Protocol Operation/Routing ***Midterm Review***
L2 IP Routing Protocols/ISP Peering, ***MIDTERM EXAM***
Lab TCP/IP Networking Lab (infrastructure components), IP Routing Protocols

Learning Objectives

Theory – After L1 and L2, students should be able to:

1. Explain the concepts of routing autonomous systems
2. Distinguish interior and exterior routing protocols
3. Understand the architectural, performance and tradeoffs of utilizing different routing protocols
4. Describe static (versus dynamic) routing
5. Explain variable length subnet masking
6. Understand the limitations of which routing protocols are able to support variable length subnet masking
7. Explain how routes (in routing) are propagated between networks
8. Explain distributed application session persistence and relationship to routing protocols and route convergence
9. Understand IP routing protocol implications in distributed application (office, data center, server farm) environments
10. Understand basic analysis tools and techniques utilized in troubleshooting distributed application performance issues
11. Explain potential impact of ISP peering and application flow between different home, business and enterprise network environments
12. Describe public peering network access points (NAPs) - Internet exchange points

Lab and Practice – After completing this lab, students should be able to:

1. Demonstrate understanding of application performance and reliability related to IP routing protocol technologies and operation.
2. Perform basic router configuration connecting different networks using interior routing protocols
3. Architect and configure end to end TCP/IP components to function on a network.
4. Apply routing concepts to home, business, enterprise connectivity to internal, external networks and **the** Internet

Week 6 Switched LAN/WAN Services

HW Comer Chapter 10, Handout (L2)
L1 LAN Switching, VLANS and VLAN Trunking
L2 Circuit/Packet/Frame switching, VPNs and tunneling
Lab VLANS, LAN Switching and VLAN Trunking

Learning Objectives

Theory – After L1 and L2, students should be able to:

1. Explain concept of switched LAN networks
2. Describe LAN switching technology
3. Describe VLANs
4. Understand concept of VLAN trunking
5. Apply VLAN concepts to enterprise connectivity services/models
6. Describe use of VLANs and trunking as secure option

Lab and Practice – After completing this lab, students should be able to:

1. Demonstrate understanding of application performance and reliability related to IP routing protocol technologies and operation.
2. Perform basic router configuration connecting different networks using interior routing protocols
3. Architect and configure end to end TCP/IP components to function on a network.
4. Apply LAN Switching, VLAN and trunking concepts to home, business, enterprise connectivity to internal, external networks and **the** Internet

Week 7 – Distributed Applications

HW Comer Chapter 22, Handouts (L1, L2)
L1 Data Center Design, VLANs, Virtualization and Cloud environments
L2 Net Application latency & performance, Network application caching/acceleration
Lab (no class/lab Nov 11 Veterans Day observed)

Learning Objectives

Theory – After L1 and L2, students should be able to:

1. Understand design and integration drivers for supporting distributed applications in data center and cloud/virtual environments
2. Describe LAN Switching, VLANs and VLAN trunking
3. Explain how VLANs are utilized in data center, cloud and enclave environments for performance and security considerations.
4. Describe connection oriented transport protocol mechanisms
5. Explain TCP congestion control operation
6. Understand retransmission timers and window management
7. Understand/describe the contributing elements and effects of latency
8. Explain application turns and relation to performance
9. Distinguish impact of bandwidth versus latency on distributed application performance
10. Understand basic analysis tools and techniques utilized in troubleshooting distributed application performance issues
11. Explain potential impact of LAN performance, routing convergence and ISP peering on distributed application systems/ environments
12. Understand TCP/IP applications SMTP, POP, IMAP for email, HTTP Telnet and SSH, FTP, FTPS, & SFTP (file transfer), XMPP – their basic use and dependencies.

Lab and Practice – After completing this lab, students should be able to:

1. Describe factors to enhance distributed application high availability
2. Describe systems level factors contributing to latency and network performance issues
3. Explain tools and techniques to effectively analyze, isolate and resolve distributed application performance issues

Week 8 – Advanced Application Services

HW Comer Chapters 19-20, Network Services Handout (L1)
Network/Application Mgmt Handout (L2)
L1 Network Svcs (QoS, Multicast, MPLS, DHCP, DNS, Active Directory, NTP, Load Balancing, Cache Servers, Content Data Networks, Accelerators)
L2 Intro networking security
Lab: Intro networking security (network ACL's) and SNMP

Learning Objectives

Theory – After L1 and L2, students should be able to:

1. Understanding the concept of Network Services
2. Explain the underlying importance of these services to your networks and distributed applications.
3. Describe how each service can be designed, built and deployed into different network environments
4. Explain the basic IP network services and their relation to distributed applications environments
5. Describe the basic goals of network management
6. Differentiate real time network diagnostics tools and network management tools collecting historical information and metrics
7. Understand Simple Network Management Protocol (SNMP) utilization in managing LANs, TCP/IP network and distributed app environments
8. Describe the key components of SNMP managed environments: managed devices, agents, and network-management systems (NMSs)
9. Understand role of Management Information Base (MIBs) in SNMP
10. Explain the utilization of SNMP tools in performance analysis, network and distributed application design

Lab and Practice – After completing this lab, students should be able to:

1. Describe network access control and protection mechanisms
2. Set up the access control lists to block TCP/IP traffic
3. Describe components and strategies in building enterprise security perimeters.

Week 9 – Wireless and Mobility

HW HW Comer Chapters 9 and 17, Handout (L1)
L1 RF Spectrum (licensed/unlicensed RF, ISM), 802.11 spec/family
L2 Wireless Architecture and Design, RFID and middleware applications
Lab Wireless Networking, Wireless Network Survey, Design and Monitoring

Learning Objectives

Theory – After L1 and L2, students should be able to:

1. Understand basic RF technology and terminology
2. Identify key characteristics of 802.11 wireless network architectures
3. Explain OSI model and IEEE 802 protocol layers in wireless LANs (WLANs)
4. Describe 802.11 MAC layer frames
5. Understand 802.11 RF channel allocation and channel reuse models
6. Describe wireless security methods and protocols
7. Understand technical requirements to support WLAN device roaming in multiple radio environment considering design/security constraints
8. Describe end to end dependencies of building WLAN systems (device, radio/RF, security, WLAN NIC etc)
9. Understand utilization and effectiveness of wireless RF surveys.
10. Describe Automated Identification Technologies (AIT) and RFID
11. Distinguish active and passive RFID technologies.
12. Explain AIT location based services
13. Describe use of middleware w/RFID systems
14. Understand how AIT/RFID can improve business productivity

Lab and Practice – After completing this lab, students should be able to:

1. Identify sources of RF contention
2. Explain WLAN design to minimize co-channel interference
3. Describe methods to design, build and monitor WLANs
4. Analyze WLAN frames and RF contention from ambient RF environments.
5. Describe technical methods to secure/protect wireless LANs

Week 10 –Network Security and Authentication

HW Comer Chapters 23-24, Handout (L1)
L1 Network encryption, VPNs, Firewalls, Network Authentication, Enterprise Security Perimeters, ***Final Exam Review***
L2 **FINAL EXAM**
Lab **NO LAB (Mon 5/30 Memorial Day Observed – holiday 2016)**

Learning Objectives

Theory – After L1 and L2, students should be able to:

1. Identify risks and threats in networked distributed application environments
2. Describe best practices for network protection and security
3. Understand role of SNMP and network tools in analyzing security related issues
4. Explain architecture and flow of enterprise security perimeters
5. Understand network authentication and its significance in supporting mobile and externally connected users and distributed applications
6. Describe network access controls
7. Understand how to utilize filters and access control lists (ACLs) for network protection mechanisms of distributed applications/resources
8. Describe application of ACLs in use case to contain SQLWorm
9. Understand technical, performance and administrative considerations of utilizing encryption in computer networks.
10. Describe technical skills required to succeed in computer network industry opportunities
11. Describe several industry network certifications (RCDD, CCNA/CCIE)
12. Explain the various requirements for each certification
13. Analyze and predict where the computer network profession is headed in the next few years

Lab and Practice – After completing this lab, students should be able to:

4. Explain the importance of networking security
5. Describe network access control and protection mechanisms
6. Set up the access control lists to block TCP/IP traffic
7. Describe components and strategies in building enterprise security perimeters.

Please read the following and sign the document:

Info 341 Computer Networks and Distributed Applications Lab Use Policy:

1. The following University of Washington lab use policy will be in effect, which can be found at: http://www.ischool.washington.edu/technology/labs/policies.aspx

2. The University of Washington acceptable computer use policy will be in effect, which can be found at: http://www.washington.edu/computing/rules/

3. Due to the special nature of the Lab Exercises for this course certain additions to the above policies will be in effect, they are the following:

- Every experiment run in conjunction with this course will have certain rules and regulations regarding its conduct. These will be explained when the assignments are given and students are expected to comply with any additional restrictions.
- To the extent that lab computers are used to stage attacks under controlled circumstances, they will be physically disconnected from all external networks. All student users of this lab must maintain this lack of connection and must verify this lack of connection (with instructor help) before running any malicious code or exploit.
- Students may be allowed to attempt to run harmful software and obtain root access on lab computers isolated from the network, as long as the students in question agree to fix any problems they cause (e.g. hardware damaging code).
- Security flaws and other problems in this lab should be pointed out immediately to the lab instructor first before calling the help desk.
- Any student running an exploit in connection with assignments in this class must file an Exploit Approval form with the instructor, before running any malicious code or attempting any exploit on any lab computer.
- Students are responsible for the consequences of any actions they take without the knowledge of the lab instructor.

I, _____, hereby certify that I have read and understand this policy and the relevant University of Washington policies referenced above regarding computer lab use and will abide by them.

Signature _____

Printed Name _____

Student ID No. _____

Dated _____

Code of Conduct

The following code of conduct has been adopted for this course:

General responsibilities for all students

Students are trusted with access to the practices, procedures and technologies used to attack and protect valuable information assets and systems. This trust requires an uncompromising commitment to satisfying the highest moral and ethical standards. Adherence to all laws, rules and regulations applicable to the field and practice of information security is critical. This requires more than simple obedience to the law. We expect that students trained by UW will demonstrate sound ethics, honesty and fairness in providing security products and services. UW expects each student to assume a sense of personal responsibility for assuring the compliance of his or her own behavior and those of their fellow students. The Code of Conduct represents a "zero tolerance" policy. All students enrolled in this course are expected to conduct their activities in a manner that satisfies the highest of ethical standards. Each student must:

- ✓ Conduct activities in accordance with high ethical and moral standards
- ✓ Conduct all activities in accordance with the academic integrity standards posted on the UHM web site
- ✓ Be aware of, and abide by, the laws of the United States, the individual States, foreign countries and other jurisdictions in which the student may conduct studies, projects, research or other activities
- ✓ Adhere to the spirit of the law as well as its substance
- ✓ Always act with personal integrity based on principles of sound judgment
- ✓ Neither condone nor ignore any illegal or unethical acts for any reason

Students should be aware that they may be held personally liable for any improper or illegal acts committed during the course of their education, and that "ignorance of the law" is not a defense. Students may be subject to civil penalties, such as fines, or regulatory sanctions, including suspension or expulsion. Potential penalties for illegal acts under federal sentencing guidelines are severe and may include imprisonment and substantial monetary fines. Existing federal and state laws, as well as the laws of foreign jurisdictions, may impose civil money penalties, permit the issuance of cease and desist orders, or have other consequences.

It is imperative that UW and its students conduct the University's academic activities in accordance with the highest possible ethical and legal standards. Every student is responsible for ensuring that his or her personal conduct is above reproach. Violations of the standards described in this Code of Conduct should be made known immediately to the instructor. UW takes these ethical obligations very seriously. Violations will not be tolerated and will result in disciplinary action appropriate to the violation.