



# Minnesota State University, Mankato HOLD and CLEAR buttons only compatible with Acrobat V. 4 and 5 Curriculum Proposal

Please type or select the requested information. Print completed forms, add appropriate paper attachments, and route through MSU's curricular process for recommendations and decisions.

(Check all that apply):		Proposal #	115
College:	Science, Engineering and Technology <input checked="" type="checkbox"/> Undergraduate	Effective Date of Change:	
Department:	Computer and Information Sciences <input checked="" type="checkbox"/> Graduate <input checked="" type="checkbox"/>	Academic Year	06-07
Program:	Computer Information science CIP # 11.0701 00	(For Office Use Only)	
Type of Change	COURSE PROPOSALS	Course Designator and Number	Number of Credits
Proposed:	New Course		
Title Current:			
Title Proposed:	Network and Security Protocols	IT 460 / IT 560	4
24-Char. Abbrev:	Network & Sec. Protocols	(if applicable)	

Include a course or program description for the Bulletin (30-40 words maximum for courses, 100 for programs):  
 Advanced coverage of data communication, networking and security protocols. Topics: transmission methods, error detection and recovery, flow control, routing, security issues and performance analysis of existing and emerging protocols for secure communication.  
 Pre: IT 214 or ISYS 215, IT 360  
 Variable

Rationale or Justification for change:  
 The CIS major is being redesigned and name changed to Information Technology (IT). This course is included in the required elective sequence for Networking and Information Security.

**\*\*\*For General Education or Cultural Diversity Courses Only\*\*\***

<b>General Education Course:</b>		<b>Cultural Diversity Course:</b>
GE Category #	GE Category Name (Maximum of 3 Categories)	(Please check one.)
N/A		<input type="checkbox"/> Core (At least 75% devoted to topics of race, gender, sexual orientation, age, class, and disabilities as they occur in United States Society.)
N/A		<input type="checkbox"/> Related (At least 25% devoted to the above topics or to a global perspective on topics related to African American, Asian, Hispanic, and Native American inhabitants of the United States.)
N/A		
? For Writing Intensive Courses, attach a description of the kind and quantity of writing. ? For Upper Division Courses, include a description of the respects in which it is broad and general rather than narrow and specific, and so suitable as GE.		
Attach paper copies of the following: a. Syllabus or course outline. b. Course's student learning outcomes associated with each GE competency or CD designation. c. List of strategies to be used to assess students' achievement of each GE competency or CD designation.		

**\*\*\*For New Courses\*\*\***

(Check all that apply):	Instructional Type: Lecture	Course will be offered:
<input checked="" type="checkbox"/> Course is an elective.	Grading Format: <input checked="" type="checkbox"/> Grade <input type="checkbox"/> P/N	<input checked="" type="checkbox"/> Fall Semester
<input type="checkbox"/> Course is required for program	Information Technology (IT)	<input checked="" type="checkbox"/> Spring Semester
<input checked="" type="checkbox"/> Pre- or Co-requisites:	IT 214 or ISYS 215, IT 360	<input type="checkbox"/> Summer Session
<input checked="" type="checkbox"/> Other courses are being changed or eliminated. (Explain.)	Minor changes in COMS 462. 462 is dropped	
<input type="checkbox"/> Course content or title is similar to courses in other departments. (Attach copy of letter of agreement with other program(s) contacted. Indicate the nature of the discussions and/or resolution of differences or potential conflicts.)		
Attach paper copies of the following: a. Syllabus or course outline. b. Course's student learning outcomes. c. A list of resources required to offer and support this course. d. A description of how teaching this course will affect department staffing. e. If 400/500 level course, an explanation of added expectations of graduate students.		



Minnesota State University, Mankato  
Curriculum Proposal

\*\*\*Signature Page\*\*\*

**Department**

Recommended (Category/ies \_\_\_\_\_)  
 Not Recommended (Category/ies \_\_\_\_\_)

David / August 10/9/06  
 Department Chair Date

Comments:

**College Curriculum Committee**

Recommended (Category/ies \_\_\_\_\_)  
 Not Recommended (Category/ies \_\_\_\_\_)

Karen C. Chou 11/2/06  
 Committee Chair Date

Comments:

**College Dean**

Recommended (Category/ies \_\_\_\_\_)  
 Not Recommended (Category/ies \_\_\_\_\_)

[Signature] 11/6/06  
 Dean Date

Comments:

**General Education Subcommittee**

Recommended (Category/ies \_\_\_\_\_)  
 Not Recommended (Category/ies \_\_\_\_\_)

\_\_\_\_\_  
 General Education Subcommittee Chair Date

Comments:

**Undergraduate Curriculum and Academic Policy Committee**

Recommended (Category/ies \_\_\_\_\_)  
 Not Recommended (Category/ies \_\_\_\_\_)

[Signature] 1-31-07  
 UCAP Faculty Chair Date

Comments:

**Faculty Association Graduate Committee**

Recommended  
 Not Recommended

\_\_\_\_\_  
 Faculty Association Graduate Chair Date

Comments:

**Graduate Dean**

Recommended  
 Not Recommended

\_\_\_\_\_  
 Graduate Dean Date

Comments:

**Academic Affairs Council**

Recommended (Category/ies \_\_\_\_\_)  
 Not Recommended (Category/ies \_\_\_\_\_)

David Flannery 2/9/07  
 Assistant Vice President Date

Comments:

**Senior Vice President and Vice President for Academic Affairs**

Approved (Category/ies \_\_\_\_\_)  
 Not Approved (Category/ies \_\_\_\_\_)

[Signature] 2/13/07  
 Sr. Vice President / Vice Pres. Academic Affairs Date

Comments:

# IT 460 (4) Network and Security Protocols

## a. SYLLABUS

### Textbook:

*Guide to TCP/IP, 2nd Ed* by Laura Chappell, Course Technology

Charlie Kaufman, Radia Perlman, and Mike Speciner, *Network Security: Private Communication in a Public World, 2nd Edition*, Prentice Hall,

*Internetworking with TCP/IP 4th ed*, by Douglas Comer, Prentice Hall

### Prerequisites:

IT 214 or ISYS 215, IT 360

### Course Objectives:

1. Acquire in depth understanding of network and security protocols.
2. Develop basic skills of secure network development through several programming assignments.
3. Employ the acquired understanding and skill in a project.

### Course Coverage:

Network protocols 55%  
Security protocols and issues 45%

### Course Contents:

Week	Topics
1	Introduction to the course, Review of Data Communications and Networking concepts, Network model, Internet Addressing, Network Security Basics
2	Data Link Layer and Network Layer protocols
3	Analysis of IP and Transport Layer Protocols
4	Application Layer Protocols and application Development
5	Domain Name System, Dynamic Host Configuration Protocol
6	Securing TCP/IP Environment, Routing in the IP environment, Managing and Monitoring IP network
7	TCP/IP and NETBIOS, IPV6
8	Wireless Networking Protocols and Security Issues
9	symmetric-key cryptography and public-key cryptography, digital signatures, internet security protocols, PGP, VPN RSA, Diffie-Hellman, and DSA algorithms.
10	IP Attacks, IP Security Protocols

11	SSL/TLS Case Study Email Security Protocols
12	Key Exchange Protocols Contract-Signing Protocols
13	Password Authentication and Key Exchange XOM architecture and security analysis
14	Symbolic Protocol Analysis Temporal logic, MOCHA, Contract-Signing
15	Protocol Logic Security in Process Calculi

### Catalog Description:

Advanced coverage of data communication, networking and security protocols. Topics include: data transmission methods, error detection and recovery, flow control, routing, data throughput, security issues, and performance analysis of existing and emerging protocols for secure communication between the many points within a computer network and across the Internet.

### Grading:

- Quizzes 15%
- Midterm 15%
- Final 20%
- Assignments 30%
- Project 20%

### b. LEARNING OUTCOMES

On completion of the course the students will be able to:

- Explain TCP/IP's history and process by which TCP/IP standards and other documents, called Requests for Comments (RFCs) are created, debated, and formalized.
- Understand and apply the basic practices and principles that underlie network protocol analysis
- Use one or more network packet capture and analysis tool
- Understand Internet addressing, anatomy and structures, public and private Internet addresses, the nature of IP address limitations, and how techniques like Classless Inter-Domain Routing (CIDR) and Network Address Translation (NAT) ease those limitations
- Understand and design *subnet* and *supernet*.
- Understand the role that data link protocols, such as SLIP (Serial Line Internet Protocol) and PPP (Point-to-Point Protocol) play for TCP/IP
- Distinguish among various Ethernet and Token Ring frame types
- Capture and analyze ARP and RARP packets to understand how hardware addresses work in a TCP/IP environment, and the services that ARP (Address Resolution Protocol) and RARP (Reverse Address Resolution Protocol) provide for such networks

- Capture and analyze IP packets to have clear understanding of IP header fields and functions including lifetime of an IP datagram, and the process of fragmentation and reassembly.
- Capture and analyze ICMP packets to understand how ICMP handles report errors, delivery errors, path discovery, Path Maximum Transmission Unit (MTU) discovery and other routing functions.
- Capture and analyze User Datagram Protocol (UDP) and Transmission Control Protocol (TCP) packets to understand their key features and functions
- Explain the mechanisms that drive segmentation, reassembly, and retransmission for the Transmission Control Protocol (TCP)
- Capture, analyze and explain the capacities, message types, and request/reply architectures for a variety of basic TCP/IP services, including FTP (File Transfer Protocol), Telnet, SMTP (Simple Mail Transfer Protocol), and HTTP (Hypertext Transfer Protocol)
- Understand the operations of other basic TCP/IP services, including Echo, Quote of the Day, Chargen, Whois, TFTP (Trivial File Transfer Protocol), Finger, Remote Procedure Call (RPC), NetBIOS services over TCP/IP (also known as NBT), and SNMP (Simple Network Management Protocol)
- Explain how to decode packets that contain Application layer protocols, and how to relate message types or other similar information to the kinds of requests and replies moving between a client and a server (or between hosts in general)
- Understand how DNS servers handle name resolution requests, including the role of nearby and root servers in the resolution process, and the difference between recursive and iterative name resolution requests
- Understand the basic services DHCP offers to its clients; explain DHCP's background, history, and origins; discuss DHCP leases; and describe the basic software components that permit DHCP to function
- Understand how basic routing works, how routing tables help control this behavior, and the various types of routing protocols, including distance vector and link-state protocols
- Understand the interior gateway protocols (such as RIP, OSPF, and EIGRP) and an exterior gateway protocol, BGP.
- Understand the anatomy of an IP attack, including the reconnaissance and discovery processes, the attack itself, and the cover-up
- Recognize common points of attacks inherent in TCP/IP architecture, explore well-known potential points for attacks on TCP/IP, and understand the form that most TCP/IP attacks usually take.
- Manually encrypt/decrypt and sign/verify signatures for small messages using RSA, Diffie-Hellman, and DSA algorithms.
- Understand symmetric-key cryptography and public-key cryptography, digital signatures, internet security protocols, PGP, VPN.
- State the requirements and mechanisms for identification and authentication.
- Explain and compare the various access control policies and models as well as the assurance of these models.
- State the characteristics of typical security architectures, including multi-level security systems.
- Explain in their own words the goals of IP Security protocols (AH and ESP), the
- Use combinations of IP security protocols to achieve a given security goal (e.g., source authentication, content authentication, traffic confidentiality, etc.)
- Explain SSL and TLS protocols.
- Apply the above protocols to protect transport-layer communication.
- State program security issues, including virus, worm, and logical bombs.
- State the basic concepts and general techniques in security auditing and intrusion detection.
- State the issues related to administration security, physical security, and program security.
- Explain the role that the Simple Network Management Protocol (SNMP) can play in an IP-based network, and understand the basic structure and function of SNMP management data, including Management Information Bases, Abstract Syntax Notation, remote monitoring, and related SNMP management objects

- Explain the limitations of IPV4 and emergence of IPV6 to overcome them including the structure and capacities of the new IPv6 address space and how it is used, IPv6 packet formats, affect on routing and features such as auto configuration, security, Quality of Service, and Mobile IP
- Understand the impediments involved in transitioning from IPv4 to IPv6, coexistence of IPv6 and IPv4, and how to use both versions simultaneously during the long transition from IPv4 to IPv6
- Write programs to send and/or receive packets and perform limited analysis task for general or specific applications.

**c. RESOURCES REQUIRED TO OFFER AND SUPPORT THIS COURSE**

Resources currently in place within the department and the University Library will support this new course. No new resources are required.

**d. IMPACT ON STAFFING IN THE DEPARTMENT**

There is no impact on department staffing.

**e. DIFFERENT ASPECT IN 500 LEVEL**

Graduate students must do independent research in a topic of current interest. Students are required to write a research paper about their topic and present their findings to the class.