

Syllabus

Course Title: Enterprise Networking

Course Number: CN 400

Course Description:

Builds on CN 321 with an analysis of the design and implementation of enterprise networks. Examines Layer 2 and 3 reliability and redundancy technologies, OSPF, TLS, QoS, congestion control, fault tolerant network designs, and SLAs.

Prerequisite Courses:

CN 321 Broadband & Wireless Fundamentals

Course Overview

Today, IT staff and network administrators must know how to design, implement, configure, operate, maintain, and extend reliable networks. There are three critical requirements of most managed organizational networks: First, a reliable network must be resilient to any single point of failure in the core devices and services, and be able to be managed and updated without significant user downtime. Second, a reliable network must protect the organization from the common attacks that are ubiquitous today, thus protecting the organizations' information resources and operations from malicious activities. Finally, when the network does go down, the design must be such that the elapsed time from failure to the restoration of services is minimized.

As an apprentice network administrator, your task is to keep the users of your network happy. As we will explore in week 1, it's all about the user ... and has nothing to do with the technology. As geeks, we love technology, and want it to be the best it can be. However that is not what the CFO wants, nor the CEO. They just want happy and productive workers who are able to use the organization's information resources.

This course has two goals to help you be a successful network administrator. The first is to extend your knowledge beyond that specific to the technologies, devices, and protocols that you learned about in your prior courses (Ethernet, 802.11, IP, TCP, ARP, etc.) to look at the network as a whole system that provides services to users. The second is to introduce the methods used today to make networks reliable and secure while enabling its use by valid users. So you must learn about users first. Then you will look at how the devices and protocols are combined with more systems and protocols (firewalls, load balancers, digital certificates, authentication services, TLS, and more) to add manageability, reliability, and security to the basic communications functionality that TCP and IP provide.

Course Outcomes:

Upon completion of this course, learners should be able to:

- Evaluate enterprise applications for their network service requirements.
- Compare Local Area Network (LAN) and Virtual LAN (VLAN) technologies as used in an enterprise network.
- Compare routing protocols (including the Enhanced Interior Gateway Routing Protocol (EIGRP) and the Open Shortest Path First (OSPF) protocol) as used in an enterprise network.
- Explain best practices when assigning IPv4 and IPv6 addresses in an enterprise network.
- Explain the role of TLS in securing data in transit.
- Summarize best practices when designing and implementing security zones in an enterprise network.
- Summarize the limitations inherent in networking technology as they affect network quality of service (QoS) metrics.
- Evaluate an enterprise network design for efficiency and effectiveness in supporting multiple locations, user device security, user content security, 24x7 availability, QoS, and congestion management.

Course Materials:

Required Texts:

Donahue, G. (2011). *Network Warrior* (2nd ed.): O'Reilly Media. ISBN 1449387861, 978-1449387860. <http://it-ebooks.info/book/435/>.

Stallings, W. (2013). *Data and Computer Communications* (10th ed.): Prentice Hall. ISBN 0133506487, 978-0133506488.

American Psychological Association. (2010). *Publication Manual of the American Psychological Association* (6th ed.). Washington, DC: American Psychological Association. ISBN 1433805618, 978-1433805615. Companion website: <http://www.apastyle.org>.

Required Resources:

Online access to textbook premium content at www.pearsonhighered.com/stallings (requires registration with student access code provided inside front cover in new textbook)

Burdach, M. (2010, Nov 2, 2010). Hardening the TCP/IP stack to SYN attacks. Symantec/SecurityFocus.com. Retrieved from <http://www.symantec.com/connect/articles/hardening-tcpip-stack-syn-attacks>

Cisco. (2005, Sept 9). IP Routing: EIGRP. Cisco Systems. Retrieved from http://www.cisco.com/en/US/tech/tk365/technologies_white_paper09186a0080094cb7.shtml

- Cisco. (2010, Aug 12). Cisco SAFE for Medium Enterprise Networks. Cisco Systems. Retrieved Feb 28, 2014, from http://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Security/SAFE_RG/safe_mediumentnetworks.html
- Colo, K. (2012, Dec 12). Using VLANs in Network Design. NEXUS, Inc. Retrieved from <http://www.spidercloud.com/assets/pdfs/VLANSecurityNexusWP1212.pdf>
- Dhillon, G. (2001). Violation of Safeguards by Trusted Personnel and Understanding Related Information Security Concerns. *Computers & Security*, 20(2), 165-172. DOI: 10.1016/S0167-4048(01)00209-7. Retrieved from [http://dx.doi.org.dml.regis.edu/10.1016/S0167-4048\(01\)00209-7](http://dx.doi.org.dml.regis.edu/10.1016/S0167-4048(01)00209-7).
- Epstein, J. (2008). Security Lessons Learned from Société Générale. *IEEE Security & Privacy*, 6(3), 80-82. DOI: 10.1109/MSP.2008.71
- Extreme Networks. (2013, Dec 11). An Overview of OpenFlow, SDNs, and OpenFlow Standards. Extreme Networks. Retrieved from <http://www.extremenetworks.com/resources/an-overview-of-openflow-sdns-openflow-standards/>
- Extreme Networks. (2014). Data Center Networking Connectivity and Topology – Design Guide. Extreme Networks. Retrieved from <http://www.extremenetworks.com/resources/data-center-networking-design-guide/> (Registration Required)
- Giachetti, R. E. (2009). Design for the Entire Business. [Article]. *Industrial Engineer*, 41(6), 39-43. Retrieved from <http://dml.regis.edu/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=bth&AN=39775659&site=ehost-live&scope=site>.
- Georgiev, M., Iyengar, S., Jana, S., Anubhai, R., Boneh, D., & Shmatikov, V. (2012). *The most dangerous code in the world: validating SSL certificates in non-browser software*. Paper presented at the Proceedings of the 2012 ACM conference on Computer and communications security, Raleigh, North Carolina, USA. <http://dl.acm.org/citation.cfm?id=2382204>.
- Leung, H. K. N. (2001). Quality metrics for intranet applications. *Information & Management*, 38(3), 137-152. DOI: 10.1016/S0378-7206(00)00060-4 Retrieved from [http://dx.doi.org.dml.regis.edu/10.1016/S0378-7206\(00\)00060-4](http://dx.doi.org.dml.regis.edu/10.1016/S0378-7206(00)00060-4).
- Levie, A. (2013, Nov 14). IT Can No Longer Afford to Ignore Its Users. *HBR Blog Network* Nov 14, 2013. Harvard Business Review. Retrieved from <http://blogs.hbr.org/2013/11/it-can-no-longer-afford-to-ignore-its-users/>
- Lopez, J., Oppliger, R., & Pernul, G. (2004). Authentication and authorization infrastructures (AAIs): a comparative survey. *Computers & Security*, 23(7), 578-590. DOI: 10.1016/j.cose.2004.06.013. Retrieved from <http://dx.doi.org.dml.regis.edu/10.1016/j.cose.2004.06.013>.

- Pepelnjak, I. (2012, May 28). Layer-2 Network Is a Single Failure Domain. IPspace. Retrieved from <http://blog.ipspace.net/2012/05/layer-2-network-is-single-failure.html?showComment=1338680223434>
- Pueblas, M., Gyurindak, S. & Strika, J. (2010). Small Enterprise Design Profile Reference Guide. Cisco Systems. Retrieved from http://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Small_Enterprise_Design_Profile/SEDP.html
- Redman, P. (2014, Jan 9). End User Computing: Thinking and Managing To The Whole Enterprise. *The Citrix Blog*. Citrix. Retrieved from <http://blogs.citrix.com/2014/01/09/end-user-computing-thinking-and-managing-to-the-whole-enterprise/>
- Shaikh, A. & Greenberg, A. (2004, Feb 7). OSPF Monitoring: Architecture, Design and Deployment Experience. AT&T Labs--Research. Retrieved from <http://www2.research.att.com/~ashaikh/papers/ospf-mon-nsdi04-html/paper.html>
- Sherman, P. J. (2009). The User Experience of Enterprise Software Matters, Part 2: Strategic User Experience. *Envision the Future*. UXMatters. Retrieved from <http://www.uxmatters.com/mt/archives/2009/03/the-user-experience-of-enterprise-software-matters-part-2-strategic-user-experience.php>
- Xipeng, X., & Ni, L. M. (1999). Internet QoS: a big picture. *Network, IEEE*, 13(2), 8-18. DOI: 10.1109/65.768484. Retrieved from <http://dx.doi.org/10.1109/65.768484>.

Optional Materials:

- Meyer, C. & Schwenk, J. (2013). Lessons Learned From Previous SSL/TLS Attacks-A Brief Chronology Of Attacks And Weaknesses. *IACR Cryptology ePrint Archive*, 2013, 49. Retrieved from <http://eprint.iacr.org/2013/049.pdf>.
- Teare, D. & Paquet, C. (2005). *Campus Network Design Fundamentals*: Cisco Press/Pearson. ISBN 1587052229, 978-1587052224.
- Vyncke, E. & Paggen, C. (2007). *Lan switch security: what hackers know about your switches*: Cisco Press. ISBN 1587052563, 9781587052569. Available via Books 24x7 & Safari Books Online.

Technology Tools:

- A personal computer with one of the following Windows operating systems: Vista or Windows 7. Wireshark will also run on Mac OS-X and Linux systems.
- Wireshark. Download and install from <http://www.wireshark.org/>.
- Lamping, Ulf, Sharpe, Richard, & Warnicke, Ed. (2011). Wireshark User's Guide. Retrieved March 3, 2011, from http://www.wireshark.org/docs/wsug_html/
- SSL Pulse. (2012, July 12). Building Together a Trustworthy Internet. Trustworthy Internet Movement. Retrieved July 24, 2012, from <https://www.trustworthyinternet.org/ssl-pulse/>

Pre-Assignment:

Online Format: Sign on to D2L (Home Page) and become familiar with the course navigation of the Web Curriculum. Read Stallings, W. (2014). Chapters 22 & 24.

Classroom-based Format: Read Stallings, W. (2014). Chapters 22 & 24.

Pre-Assignment Due Dates:

Classroom-based Format: This assignment is due the first night of class.

Online Format: The instructor will specify the due date for this assignment.

Course Assignments and Activities:

	Topics	Readings	Activities Assignments and Associated Points
1	User Expectations from an Enterprise Network	<ul style="list-style-type: none">Stallings, W. (2014). Chapters 22, 24.From the Experts	Class Discussion: <ul style="list-style-type: none">IntroductionsDiscussion Questions (50 pts)
2	Implementing Layer 2 in Practice	<ul style="list-style-type: none">Donahue, G. A. (2011). Chapters 4, 5, 6, 8From the Experts	Class Discussion: <ul style="list-style-type: none">Discussion Questions (50 pts) Written Assignment: <ul style="list-style-type: none">Simple LAN Evaluation (100 pts)
3	Implementing Layer 2 Redundancy	<ul style="list-style-type: none">Donahue, G. A. (2011). Chapters 7, 13, 14From the Experts	Class Discussion: <ul style="list-style-type: none">Discussion Questions (50 pts) Written Assignment: <ul style="list-style-type: none">Reliable LAN Evaluation (100 pts)
4	Implementing Layer 3	<ul style="list-style-type: none">Donahue, G. A. (2011). Chapters 9, 10, 36, 37Stallings, W. (2014). Chapters 14, 19 (Review as needed given your background)From the Experts	Class Discussion: <ul style="list-style-type: none">Discussion Questions (50 pts) Written Assignment: <ul style="list-style-type: none">IP Address Map (100 pts)
5	Enterprise Network Security	<ul style="list-style-type: none">Donahue, G. A. (2011). Chapters 25, 27Stallings, W. (2014). Chapters 27 (see publisher's website)From the Experts	Class Discussion: <ul style="list-style-type: none">Discussion Questions (50 pts) Written Assignment: <ul style="list-style-type: none">Access Control Lists (100 pts)
6	TLS, Digital Certificates, and Authentication Infrastructures	<ul style="list-style-type: none">From the Experts	Class Discussion: <ul style="list-style-type: none">Discussion Questions (50 pts) Written Assignment: <ul style="list-style-type: none">Virtual Lab – Capture a TLS Connection Setup (100 pts)

7	Quality of Service & Congestion Management	<ul style="list-style-type: none"> • Donahue, G. A. (2011). Chapters 31, 32, 33, 34 • Stallings, W. (2014). Chapters 20 (see publisher's website) • From the Experts 	Class Discussion: <ul style="list-style-type: none"> • Discussion Questions (50 pts) Written Assignment: <ul style="list-style-type: none"> • Evaluating for QoS Effectiveness (100 pts)
8	Enterprise Network Design Issues	<ul style="list-style-type: none"> • Donahue, G. A. (2011). Chapters 35 • From the Experts 	Class Discussion: <ul style="list-style-type: none"> • Discussion Questions (50 pts)
			Maximum Points Possible: 1000

Course Policies and Procedures:

CC&IS Grading Scale

Letter Grade	Percentage	Grade Point
A	93 to 100	4.00
A-	90 to less than 93	3.67
B+	87 to less than 90	3.33
B	83 to less than 87	3.00
B-	80 to less than 83	2.67
C+	77 to less than 80	2.33
C	73 to less than 77	2.00
C-	70 to less than 73	1.67
D+	67 to less than 70	1.33
D	63 to less than 67	1.00
D-	60 to less than 63	.67
F	Less than 60	0

Additional information about grading can be found in the latest edition of the University Catalog, available at <http://www.regis.edu/Academics/Course%20Catalog.aspx>.

CC&IS Policies and Procedures

Each of the following CC&IS Policies & Procedures is incorporated here by reference. Students are expected to review this information each term, and agree to the policies and procedures as identified here and specified in the latest edition of the University Catalog, available at <http://www.regis.edu/Academics/Course%20Catalog.aspx> or at the link provided.

- The CC&IS Academic Integrity Policy.
- The Student Honor Code and Student Standards of Conduct.
- Incomplete Grade Policy, Pass / No Pass Grades, Grade Reports.

- The Information Privacy policy and FERPA. For more information regarding FERPA, visit the [U.S. Department of Education](#).
- The HIPAA policies for protected health information. The complete Regis University HIPAA Privacy & Security policy can be found here: <http://www.regis.edu/About-Regis-University/University-Offices-and-Services/Auxiliary-Business/HIPAA.aspx>.
- The Human Subjects Institutional Review Board (IRB) procedures. More information about the IRB and its processes can be found here: <http://regis.edu/Academics/Academic-Grants/Proposals/Regis-Information/IRB.aspx>.

The CC&IS Policies & Procedures Syllabus Addendum summarizes additional important policies including, Diversity, Equal Access, Disability Services, and Attendance & Participation that apply to every course offered by the College of Computer & Information Sciences at Regis University. A copy of the CC&IS Policies & Procedures Syllabus Addendum can be found here: <https://in2.regis.edu/sites/ccis/policies/Repository/CCIS%20Syllabus%20Addendum.docx>.