

## Washtenaw Community College Comprehensive Report

### CNT 217 CCNA Security Certification Proposed Start Semester: Winter 2011

#### Course Cover

**Division:** Business and Computer Technologies  
**Department:** Computer Instruction  
**Discipline:** Computer Networking Technology  
**Course Number:** 217  
**Org Number:** 13400  
**Full Course Title:** CCNA Security Certification  
**Transcript Title:** CCNA Security Certification  
**Is Consultation with other department(s) required:** No  
**Publish in the Following:** College Catalog , Time Schedule , Web Page  
**Reason for Submission:** New Course  
**Change Information:**  
**Rationale:** Conditionally approved; seeking full approval.  
**Proposed Start Semester:** Winter 2011

**Course Description:** This course prepares students for the Cisco Certified Network Associate (CCNA) Security certification examination. The course provides students with the knowledge and hands-on skills necessary to install, configure and monitor Cisco security devices.

#### Course Credit Hours

**Variable hours:** No  
**Credits:** 4  
**Lecture Hours: Instructor: 60 Student: 60**  
**Lab: Instructor: 0 Student: 0**  
**Clinical: Instructor: 0 Student: 0**  
**Other: Instructor: 0 Student: 0 Total Contact Hours: Instructor: 60 Student: 60**  
**Repeatable for Credit:** NO  
**Grading Methods:** Letter Grades  
 Audit  
**Are lectures, labs, or clinicals offered as separate sections?:** NO (same sections)

#### College-Level Reading and Writing

College-level Reading & Writing

#### Requisites

**Prerequisite**  
 CNT 236 minimum grade "C"; may enroll concurrently  
 or equivalent industry experience  
**Prerequisite**  
 Academic Reading and Writing Levels of 6

#### General Education

#### Request Course Transfer

**Proposed For:**

#### Student Learning Outcomes

1. Identify network threats, mitigation techniques, and the basics of securing a network.

*logged 9/8/10 sj*

**Assessment 1****Assessment Tool:** Cisco-developed final concepts exam**Assessment Date:** Winter 2014**Assessment Cycle:** Every Three Years**Course section(s)/other population:** Minimum of two sections over the three year period.**Number students to be assessed:** All**How the assessment will be scored:** External evaluation.**Standard of success to be used for this assessment:** At least 80% of students must score 75% or better.**Who will score and analyze the data:** The assessment is scored at the Cisco Academy site. Department faculty analyze the results.

2. Secure administrative access on routers and switches.

**Assessment 1****Assessment Tool:** Cisco-developed final skills exam**Assessment Date:** Winter 2014**Assessment Cycle:** Every Three Years**Course section(s)/other population:** Minimum of two sections over the three year period.**Number students to be assessed:** All**How the assessment will be scored:** External evaluation.**Standard of success to be used for this assessment:** At least 80% of students must score 75% or better.**Who will score and analyze the data:** The assessment is scored at the Cisco Academy site. Department faculty analyze the results.

3. Protect networks by using firewalls and intrusion prevention systems.

**Assessment 1****Assessment Tool:** Cisco-developed final skills exam**Assessment Date:** Winter 2014**Assessment Cycle:** Every Three Years**Course section(s)/other population:** Minimum of two sections over the three year period.**Number students to be assessed:** All**How the assessment will be scored:** External evaluation.**Standard of success to be used for this assessment:** At least 80% of students must score 75% or better.**Who will score and analyze the data:** The assessment is scored at the Cisco Academy site. Department faculty analyze the results.

4. Prevent unauthorized insider access to networks by using layer 2 authentication.

**Assessment 1****Assessment Tool:** Cisco-developed final skills exam**Assessment Date:** Winter 2014**Assessment Cycle:** Every Three Years**Course section(s)/other population:** Minimum of two sections over the three year period.**Number students to be assessed:** All**How the assessment will be scored:** External evaluation.**Standard of success to be used for this assessment:** At least 80% of students must score 75% or better.**Who will score and analyze the data:** The assessment is scored at the Cisco Academy site. Department faculty analyze the results.

5. Implement router-based virtual private networks (VPNs).

**Assessment 1****Assessment Tool:** Cisco-developed final skills exam**Assessment Date:** Winter 2014

**Assessment Cycle:** Every Three Years

**Course section(s)/other population:** Minimum of two sections over the three year period.

**Number students to be assessed:** All

**How the assessment will be scored:** External evaluation.

**Standard of success to be used for this assessment:** At least 80% of students must score 75% or better.

**Who will score and analyze the data:** The assessment is scored at the Cisco Academy site. Department faculty analyze the results.

## Course Objectives

1. Describe attack vectors to networks and devices.

### **Methods of Evaluation**

Activity or Exercise

Exams/Tests

Lab Activity, Report or Test

Quizzes

### **Matched Outcomes**

1. Identify network threats, mitigation techniques, and the basics of securing a network.

2. Describe attack vectors to networks and devices.

### **Methods of Evaluation**

Activity or Exercise

Lab Activity, Report or Test

### **Matched Outcomes**

2. Secure administrative access on routers and switches.

3. Configure local and AAA authentication on routers and switches.

### **Methods of Evaluation**

Activity or Exercise

Exams/Tests

Lab Activity, Report or Test

Quizzes

### **Matched Outcomes**

3. Protect networks by using firewalls and intrusion prevention systems.

4. Configure dynamic and reflexive access control lists to mitigate against attacks.

### **Methods of Evaluation**

Activity or Exercise

Exams/Tests

Lab Activity, Report or Test  
Quizzes

**Matched Outcomes**

3. Protect networks by using firewalls and intrusion prevention systems.

5. Configure a Context-Based and a Zone-Based Policy Firewall.

**Methods of Evaluation**

Activity or Exercise  
Exams/Tests  
Lab Activity, Report or Test  
Quizzes

**Matched Outcomes**

3. Protect networks by using firewalls and intrusion prevention systems.

6. Configure and monitor an Intrusion Prevention System.

**Methods of Evaluation**

Activity or Exercise  
Exams/Tests  
Lab Activity, Report or Test  
Quizzes

**Matched Outcomes**

3. Protect networks by using firewalls and intrusion prevention systems.

7. Describe different types of Intrusion Prevention Systems.

**Methods of Evaluation**

Activity or Exercise  
Exams/Tests  
Lab Activity, Report or Test  
Quizzes

**Matched Outcomes**

4. Prevent unauthorized insider access to networks by using layer 2 authentication.

8. Describe layer 2 attacks against switches and devices.

**Methods of Evaluation**

Activity or Exercise

Exams/Tests  
 Lab Activity, Report or Test  
 Quizzes

**Matched Outcomes**

1. Identify network threats, mitigation techniques, and the basics of securing a network.
  
4. Prevent unauthorized insider access to networks by using layer 2 authentication.
  
9. Configure switches to mitigate against layer 2 attacks.

**Methods of Evaluation**

Activity or Exercise  
 Exams/Tests  
 Lab Activity, Report or Test  
 Quizzes

**Matched Outcomes**

1. Identify network threats, mitigation techniques, and the basics of securing a network.
  
5. Implement router-based virtual private networks (VPNs).
  
10. Describe the different types of encryption protocols.

**Methods of Evaluation**

Activity or Exercise  
 Exams/Tests  
 Lab Activity, Report or Test  
 Quizzes

**Matched Outcomes**

1. Identify network threats, mitigation techniques, and the basics of securing a network.
  
5. Implement router-based virtual private networks (VPNs).
  
11. Describe the differences between symmetric and asymmetric encryption algorithms.

**Methods of Evaluation**

Activity or Exercise  
 Exams/Tests  
 Lab Activity, Report or Test  
 Quizzes

**Matched Outcomes**

5. Implement router-based virtual private networks (VPNs).
  
12. Configure an IPsec virtual private network using routers.

**Methods of Evaluation**

Activity or Exercise  
Exams/Tests  
Lab Activity, Report or Test  
Quizzes

**Matched Outcomes**

5. Implement router-based virtual private networks (VPNs).

**New Resources for Course**

**Course Textbooks/Resources**

Textbooks

Manuals

Cisco Press. CCNA Security Lab Manual, Cisco Press 1-58713-249-4, 08-03-2009

Periodicals

Software

Other

**Equipment/Facilities**

Computer workstations/lab

---