Academic Catalog | 2022

Academic Catalog

ALL TRADEMARKS ENCLOSED WITHIN THIS PUBLICATION
ARE THE PROPERTY OF THE RESPECTIVE COMPANY.

For January 01, 2022 – December 31, 2022

Brand College
529 Hahn Ave. Suite 101 ♦ Glendale CA 91203-1052
Tel 818.550.0770 ♦ Fax 818.550.8293
www.brandcollege.edu

Table of Contents

MISSION AND OBJECTIVES ---- 3

HISTORY ---- 4

INDUSTRY AFFILIATIONS ---- 5

Technic Affiliations ---- 5
Educational Affiliations ---- 5

SCHOOL OVERVIEW ---- 6

GENERAL INFORMATION ---- 7

Facilities ---- 7
Campus Information ---- 8

ADMISSIONS REQUIREMENTS ---- 9

Procedures ---- 9
Schedule of Total Charges ---- 11
Clock Hour Conversion ---- 14
Language ---- 14

TUITION AND REFUND POLICY ---- 15

Installment Contract ---- 15
"Student's Right to Cancel" ---- 15
Cancellation of Agreement ---- 15
Withdrawal From Course ---- 15
Hypothetical Refund Example ---- 16
Disclosure ---- 17

ACADEMIC POLICIES ---- 19

Satisfactory Academic Progress - Description ---- 19
Satisfactory Academic Progress – Process Flow ---- 21
Attendance ---- 22
Tardiness ---- 22
Make-Up Works ---- 22
Student Code of Conducts ---- 23
Disciplinary Dismissal ---- 23
Conditions for Re-Enrollment ---- 23
Grading System ---- 23
Student's Records ---- 24
Complaint Policies and Procedure ---- 24
Student Complaint Procedure ---- 24
Graduation Requirements ---- 25

BRAND COLLEGE SERVICES ---- 26

Student Services ---- 26
Placement Services ---- 27

ACADEMIC PROGRAMS ---- 29

Cisco Certified Network Associate (CCNA) ---- 29
Cisco Certified Network Professional (CCNP) ---- 41
Cisco Certified Network Expert (CCNE) ---- 46
Certified Network Technologies Expert (CNTE) ---- 76

2022 – 2023 ACADEMIC CALENDAR ---- 106

Mission and Objectives

The primary mission of Brand College is to provide students with high quality, career oriented educational programs. Our goal is to ensure that students receive the highest possible standard of education in their field of study. At Brand College, we have made every effort to create the optimum environment in which students gain real-life experiences in the classroom. We aim to prepare our students to be fully capable to work "in the field". The education students receive at Brand College will greatly enhance their chances of securing the best possible employment in their field of study.

Students will benefit from our dedication to excellence in training, and our continuous efforts to provide the following:

- Personal, hands-on education.
- Ample class time, above and beyond the requirements, to ensure our students get a chance to absorb the material thoroughly, ask questions and practice through lab exercises.
- Small class sizes for individual attention.
- Instructors who have extensive real-life experience and a passion for training.
- Google Classroom is Brand College's Course Management System (CMS) for asynchronous learning and Google Meet as its online video conferencing platform for synchronous instructions. Both platforms are developed and managed by Google and are trusted by public and private schools alike. Google's engineering and operations expertise deliver a very reliable and highly available infrastructure through committed levels of managed services as well as a highly secure platform for schools and students. This in turn allows Brand College to focus on its core mission of ensuring that students receive the highest possible standard of education without the need to develop and maintain an online learning system. In turn, the students are enabled to access the Course Management System (CMS) and meet in real-time video conferencing sessions for their class utilizing only an internet browser on the device of their choice.

Now, more than ever, businesses have begun to demand industry certified employees who are qualified to plan, install, operate, maintain, and support today's complex computer environments. As the computer market enters into a new era of automation, business needs are being re-evaluated to take advantage of the new technologies that are far more complex, sophisticated, require support personnel with advanced training and skills. With these changes, highly qualified individuals will be needed to allow organizations to improve their overall operations. With increased computerization and automation of the business environment, computer training has become a needed commodity in this ever-changing field. As technology rapidly advances, it is apparent that well-educated and highly trained personnel are in demand to manage and operate this growing computing platform.

The areas of need will range from training for basic software skills to highly technical training on how to develop and maintain computer systems for large and growing organizations and enterprises.

The above needs simply illustrate that there is a vast pool of candidates eligible for Brand College's programs. Candidates will range from individuals just starting in the field of technology to those experienced and technical personnel wanting to upgrade or update their skills.

History

Brand College was established in 2004 in Glendale, California, as a Limited Liability Corporation.

Brand College, a private institution, that is approved to operate by the Bureau, and that approval to operate means compliance with state standards as set forth in the CEC and 5,CCR. An institution may not imply that the Bureau endorses programs, or that Bureau approval means the institution exceeds minimum state standards. (CEC 94909 (a)(2) and 94897 (I)(1)(2))

Any questions a student may have regarding this catalog that have not been satisfactorily answered by the institution may be directed to the Bureau for Private Postsecondary Education at:

1747 N. Market Blvd., Suite 225
Sacramento, CA 95834

P.O. Box 980818
West Sacramento, CA 95798-0818

www.bppe.ca.gov
Toll free telephone number (888) 370-7589
or by fax (916) 263-1897

The primary focus of the organization is to provide quality training to its clients in the area of Information Technology and related studies. The organization currently has four (4) partners and will be operating out of its headquarters in Glendale, California. The company offers its customers a unique combination of expertise – comprehensive and practical Information Technology training in many of the sought-after programs in the industry.

The primary mission of the organization is to provide students with high quality, career oriented programs. Our goal is to ensure that students receive the highest possible standard of education in their field of study. At Brand College, we have made every effort to create the optimum environment in which students gain real-life experiences in the classroom. We aim to prepare our students to be fully capable to work "in the field". The education students receive at Brand College will greatly enhance their chances of securing the best possible employment in their field of study.

Our educational services include:

1. Certification training programs including:
    a. Cisco Certified Network Associate (CCNA),
    b. Cisco Certified Network Professional (CCNP)
2. Comprehensive programs including:
    a. Cisco Certified Network Expert (CCNE),
    b. and Certified Network Technologies Expert (CNTE);
3. Skill and knowledge enhancement training not specifically linked to certifications including:
    a. Security training for firewall and VPN solutions,
    b. End-user and corporate training directed at updating employee/user skill set and knowledge base,
    c. Certification preparation,
    d. and certification testing.

Industry Affiliations

Brand College is proud to honor affiliations with industry and educational leaders while it continues to expand its partnerships, certifications, and/or memberships:

Technic Affiliations

- VMWare IT Academy
- Palo Alto IT Academy

Educational Affiliations

- Brand College is accredited by the Accrediting Commission of Career Schools and Colleges (ACCSC)
- Brand College is licensed to operate by BPPE. For more information visit www.bppe.ca.gov
- Pearson VUE Testing Center
- Dun and Bradstreet

School Overview

We believe a key element to the future success of Brand College will be the quality of its personnel. The team of individuals that is to become Brand College is comprised of a balanced blend of engineers, instructors, business managers, and administrators. Each member of the organization brings a high level of expertise and experience to the team. Additionally, the group has already attracted a number of highly regarded outside contractors and professional support personnel. Brand College is a cohesive group of talented, energetic, individuals fully prepared to build a highly successful, well regarded, IT company.

Brand College has no pending petition in bankruptcy, is not operating as a debtor in possession, has not filed a petition within the preceding five years, or has not had a petition in bankruptcy filed against it within the preceding five years that resulted in reorganization under Chapter 11 of the United States Bankruptcy Code (11 U.S.C. Sec. 1101 et seq.).

General Information

Facilities

Brand College is located in Glendale, California at 529 Hahn Avenue, near the heart of the Glendale business district. The facilities can be found on the first floor of a two-story building. The space occupied by school is approximately 1,340 square feet.

The space consists of two classrooms/labs, a student lounge area, administrative offices, Pearson VUE Testing Center, and a library/resource center.

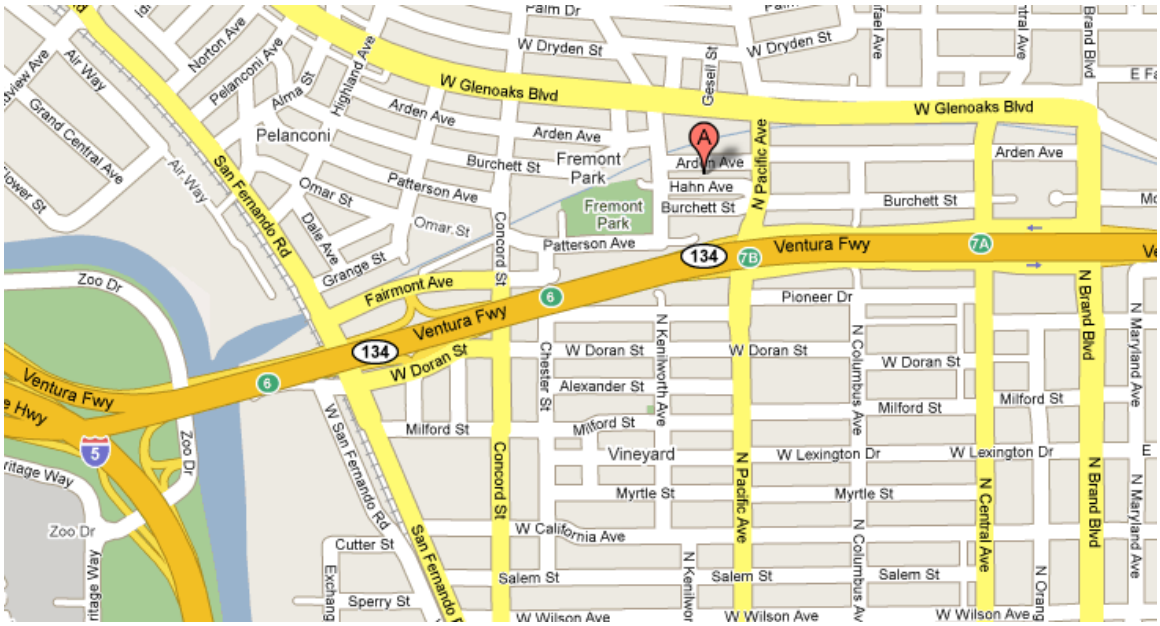
The classrooms/lab 1 accommodates up to 16 students while the classroom/lab 2 can accommodate up to 12 students. Both classroom/labs provide a student to computer ratio of 1:1, equipped with up-to-date computer equipment.

School's labs are equipped with hardware, software and network infrastructure as required by training programs.

All areas of the facility are well lighted and well ventilated. Additionally, the west side of the building is banked by large windows allowing for pleasant, natural lighting into a significant portion of the suites.

Campus Information

Brand College
529 Hahn Ave. Suite 101
Glendale, CA 91203-1052



Admissions Requirements

To be admitted to any program at Brand College, applicants must provide one of the following documents, prior to start of the program.

1. Copy or original high school transcript indicating the applicant fulfilled the requirements for graduation from high school.
2. Copy or original recognized equivalency certificate such as the General Education Development (GED) or copy or original GED transcript showing fulfillment of the requirements for a GED.
3. Copy or original applicant's high school diploma, associate degree, bachelor's degree or master's degree.
4. Copy or original of postsecondary school academic transcript which gives proof to one of the following: completed associate, bachelor or master's degree.
5. All applicants from foreign, non-English speaking countries must provide above documentation that is to be translated and certified to be at least equivalent to a U.S. high school diploma. The agency should be a member of the National Association of Credential Evaluation Services (NACES) or Association of International Credential Evaluators (AICE).
6. All applicants must pass an entrance exam given by the college before the start of class. The entrance exam entails assessment for basic writing and reading for English proficiency.

Brand College's programs entail rigorous computer-based training requiring basic computer knowledge, logic and reasoning abilities, mathematics aptitude, and writing skills. In order to accurately evaluate an applicant's ability to succeed in this training program, prospective students have to successfully pass school's entrance exam. The Wonderlic is a designated exam for Brand College. Score of at least 12 will be required for an applicant to be considered for admission to school. The exam may not be repeated within a seven-day period in the event the applicant does not pass the exam.

As a prospective student, you are encouraged to review this catalog prior to signing an enrollment agreement. You are also encouraged to review the School Performance Fact Sheet, which must be provided to you prior to signing an enrollment agreement.

Brand College encourages students to review the catalog and School Performance Fact Sheet prior to signing the school's enrollment agreement.

Procedures

To apply for admission, applicants are required to pass school's interview process and entrance exam as described below.

Applicants are required to interview with one of our Admissions Representatives. Based on the interview responses, school's panel members discuss the applicant's background, interest, and future plans in applicant's area of interest. Current job market analysis is referenced and considered in determining the needs and interest of the applicant. Applicants are also given a tour of school's facility.

If school's program is deemed beneficial and suitable for the applicant, and the applicant is interested in enrolling in the offered program, then the applicant is required to pass school's entrance exam. The entrance exam entails assessment for basic writing and reading for English proficiency. Applicants should also be prepared to present a copy of their diploma or GED along with the required registration fee.

Upon acceptance into the school, the applicant will complete an enrollment agreement that outlines applicant's financial responsibility.

If the school rejects the applicant, he/she will be notified immediately, and all sums paid as part of the program tuition will be fully refunded to the student.

Distance Education Admission Procedures

Brand College's delivery of learning programs via distance education does not alter the assessment criteria and methodology to ensure the appropriateness of the programs for students. That is primarily attributed to the following.

- Brand College continues to adhere to and comply with student assessment and admission policies to which ACCSC granted approval to Brand College for its residential programs.
- Brand College's distance education programs are the approved residential programs by ACCSC.
- Brand College continues to only enroll students who based on their location are able to attend classes in person should residential classes be offered during their enrollment period.
- Brand College conducts the student assessment in person at the school's campus.

Schedule of Total Charges

Program	Tuition, Books, and Equipment
Cisco Certified Network Associate	$2,500.00
Cisco Certified Network Professional	$7,500.00
Certified Network Technologies Expert	$31,000.00
Cisco Certified Network Expert	$20,000.00

The school reserves the right to adjust tuition rates. In no event will any such changes affect the students that already have signed an enrollment agreement with the school.

1. The charges for period of attendance and the total charges for the entire program are the same
2. Total charges for each program include textbooks, equipment, and or any material needed.
3. Brand College is eligible but chooses not to participate in Federal or State Student Aid Programs.

76215. Student Tuition Recovery Fund Disclosures

(a) A qualifying institution shall include the following statement on both its enrollment agreement and school catalog:
"The State of California established the Student Tuition Recovery Fund (STRF) to relieve or mitigate economic loss suffered by a student in an educational program at a qualifying institution, who is or was a California resident while enrolled, or was enrolled in a residency program, if the student enrolled in the institution, prepaid tuition, and suffered an economic loss. Unless relieved of the obligation to do so, you must pay the state-imposed assessment for the STRF, or it must be paid on your behalf, if you are a student in an educational program, who is a California resident, or are enrolled in a residency program, and prepay all or part of your tuition.

You are not eligible for protection from the STRF and you are not required to pay the STRF assessment, if you are not a California resident, or are not enrolled in a residency program."

(b) In addition to the statement required under subdivision (a) of this section, a qualifying institution shall include the following statement in its school catalog:

"It is important that you keep copies of your enrollment agreement, financial aid documents, receipts, or any other information that documents the amount paid to the school. Questions regarding the STRF may be directed to the Bureau for Private Postsecondary Education, 1747 N. Market Blvd., Suite 225, Sacramento, CA 95834, (916) 574-8900 or (888) 370-7589.

To be eligible for STRF, you must be a California resident or are enrolled in a residency program, prepaid tuition, paid or deemed to have paid the STRF assessment, and suffered an economic loss as a result of any of the following:
1. The institution, a location of the institution, or an educational program offered by the institution was closed or discontinued, and you did not choose to participate in a teach-out plan approved by the Bureau or did not complete a chosen teach-out plan approved by the Bureau.
2. You were enrolled at an institution or a location of the institution within the 120 day period before the closure of the institution or location of the institution, or were enrolled in an educational program within the 120 day period before the program was discontinued.
3. You were enrolled at an institution or a location of the institution more than 120 days before the closure of the institution or location of the institution, in an educational program offered by the institution as to which the Bureau determined there was a significant decline in the quality or value of the program more than 120 days before closure.
4. The institution has been ordered to pay a refund by the Bureau but has failed to do so.
5. The institution has failed to pay or reimburse loan proceeds under a federal student loan program as required by law, or has failed to pay or reimburse proceeds received by the institution in excess of tuition and other costs.
6. You have been awarded restitution, a refund, or other monetary award by an arbitrator or court, based on a violation of this chapter by an institution or representative of an institution, but have been unable to collect the award from the institution.
7. You sought legal counsel that resulted in the cancellation of one or more of your student loans and have an invoice for services rendered and evidence of the cancellation of the student loan or loans.

To qualify for STRF reimbursement, the application must be received within four (4) years from the date of the action or event that made the student eligible for recovery from STRF.

A student whose loan is revived by a loan holder or debt collector after a period of noncollection may, at any time, file a written application for recovery from STRF for the debt that would have otherwise been eligible for recovery. If it has been more than four (4) years since the action or event that made the student

eligible, the student must have filed a written application for recovery within the original four (4) year period, unless the period has been extended by another act of law.

However, no claim can be paid to any student without a social security number or a taxpayer identification number."

Clock Hour Conversion

- Term- Quarter (12 weeks)
- Classroom/Laboratory Contact Hour – Fifty (50) minutes of class time
- One Quarter Credit Hour - Twelve (12) hours of classroom contact plus appropriate outside preparation
- One Quarter Clock Hour - Twenty-four (24) hours of supervised laboratory instruction plus appropriate outside preparation

Language

Brand College only offers classes in English. We do not offer ESL classes.

Tuition and Refund Policy

Installment Contract

Installment of more than four (4) payments requires the completion and execution of Brand College's Promissory Note – Tuition Assistance agreement in addition to this Enrollment Agreement. Student (and Co-buyer, if applicable) understands that payments are made to the School (Brand College). Payments 10 days delinquent may accrue a LATE CHARGE of the lesser of 5%, $5 or maximum allowed by law. If account is delinquent for over 90 days, the entire amount may become due and payable. I/we Student (and Co-buyer, if applicable), agree to pay all funds owed under this agreement to the school on demand. I/we Student (and Co-buyer, if applicable), do not, I/we agree to pay all costs of collection, including attorney and collection agency costs in addition to what I/we owe. The Agreement is not binding until accepted by the School. Student may pay off balance in advance (within 90 days of start date) and receive partial refund of interest computed by the actuarial method. **NOTICE: "YOU MAY ASSERT AGAINST THE HOLDER OF THE PROMISSORY NOTE YOU SIGNED IN ORDER TO FINANCE THE COST OF THE EDUCATIONAL PROGRAM ALL OF THE CLAIMS AND DEFENSES THAT YOU COULD ASSERT AGAINST THIS INSTITUTION, UP TO THE AMOUNT YOU HAVE ALREADY PAID UNDER THE PROMISSORY NOTE."**

"Student's Right to Cancel"

Cancellation of Agreement

You have the right to cancel this agreement for a course of instruction including any equipment such as books or any other goods related to the instruction offered in this agreement, through attendance at the first class session or until midnight of the seventh (7) business day after enrollment, whichever is later. Student has the right to obtain a refund of charges paid through attendance at the first class session, or the seventh day after enrollment, whichever is later.

Cancellation shall occur when you give written notice of cancellation at the address of the School shown on the top of the front and back page of this agreement. You can do this by mail, hand delivery, or telegram. The written notice of cancellation, if sent by mail, is effective when deposited in the mail properly addressed with postage prepaid. The written notice of cancellation need not take any particular form and, however expressed, it is effective if it shows that you no longer wish to be bound by agreement. You will be given two Notice of Cancellation forms to use at the first day of class, but you can use any written notice that you wish.

If the school has given you any equipment, including books or other materials, you shall return it to the school within 30 days following the date of your notice of cancellation. If you fail to return this equipment, including books, or other materials, in good condition within a 30-day period, the school may deduct its documented cost for the equipment from any refund that may be due to you. Once you pay for the equipment, it is yours to keep without further obligation. If you cancel this agreement, the school will refund any money that you paid, less any deduction for equipment not timely returned in good condition, within 30 days after your notice of cancellation is received.

Withdrawal From Course

You have the right to withdraw from a course of instruction at any time. If you withdraw from the course of instruction after the period allowed for cancellation of the agreement, which is until midnight of the seventh (7) business day following the first class you attended, the school will remit a refund less a registration fee, if applicable, not to exceed $75.00 within 30 days following your withdrawal. You are obligated to pay only for education services rendered and for unreturned equipment. The refund shall be the amount you paid for instruction, less a registration fee, multiplied by a fraction in which the numerator is the number of hours of instruction which you have not received but for which you have paid, and the denominator is the total number of hours of instruction for which you have paid. If you obtain equipment,

as specified in the agreement as a separate charge, and return it in good condition within 30 days following the date of your withdrawal, the school shall refund the charge for equipment paid by you. If you fail to return the equipment in good condition, allowing for reasonable wear and tear, within 30 days period, the school may offset against the refund the documented cost to the school of that equipment. You shall be liable for the amount, if any, by which the documented cost for equipment exceeds the prorated refund amount. The documented cost of the equipment may be less than the amount charged, and the amount the school has charged in the contract.

In any event, you will never be charged for more than the equipment charges stated in the contract. For a list of these charges, see the list on the front of this page. IF THE AMOUNT THAT YOU HAVE PAID IS MORE THAN THE AMOUNT THAT YOU OWE FOR THE TIME YOU ATTENDED, THEN REFUND WILL BE MADE WITHIN 30 DAYS OF WITHDRAWAL. IF THE AMOUNT THAT YOU OWE IS MORE THAN THE AMOUNT THAT YOU HAVE ALREADY PAID, THEN YOU WILL HAVE TO MAKE ARRANGEMENTS TO PAY IT.

An approved leave of absence (LOA) is not considered to be a withdrawal of the student which requires a refund. A LOA is approved if, (1) the student has made a written request for the LOA, (2) the leave of absence does not exceed sixty (60) days, (3) the school has granted only one LOA to the student in any 12-month period, and (4) the school does not charge the student for the LOA. If the LOA is not approved then the student is considered withdrawn from the school, and the refund requirements apply.

Hypothetical Refund Example
Assume the student has paid in full the following charges for a 400-hour course:

Registration Fee:	$75.00
Tuition:	$2,025.00
Equipment:	$150.00

(student has received all necessary equipment)

Student withdraws from the school after 100 hours of instruction. The pro rata refund for the student would be:

(2025 x 300) / 400 = 1518.75 (refund of $1,518.75)

If the student returns the equipment in good condition within 10 days following his/her withdrawal, the school shall refund the charge for the equipment paid by the student. Thus the refund amount will be:

$1,518.75 + $150 = $1,668.75

For the purpose of determining the amount you owe for the time you attended, you shall be deemed to have withdrawn from the course when any of the following occurs:

(a) You notify the school of your withdrawal or the actual date of withdrawal.
(b) The school terminates your enrollment. **
(c) You fail to attend classes for a three-week period. In this case, the date of withdrawal shall be the last date of recorded attendance.
(d) You fail to submit three consecutive lessons or you fail to submit a completed lesson required for home study or correspondence within 60 days of its due date.

If a student obtains a loan to pay for an educational program, the student will have the responsibility to repay the full amount of the loan plus interest, less the amount of any refund, and that, if the student has received federal student financial aid funds, the student is entitled to a refund of the moneys not paid from federal student financial aid program funds. If the student obtained a loan guaranteed by the federal or

state government and the student defaults on the loan, both of the following may occur: (1) The federal or state government or a loan guarantee agency may take action against the student, including applying any income tax refund to which the person is entitled to reduce the balance owed on the loan. (2) The student may not be eligible for any other federal student financial aid at another institution or other government financial assistance until the loan is repaid.

******<u>*Grounds for cancellation/termination by the school*</u> *– failure to maintain satisfactory academic progress, excessive unexcused absences, violation of school Codes of Conduct, and/or failure to meet financial obligations to the school.*

Disclosure

The school reserved the right to cancel a class start date due to insufficient enrollment. If this occurs, the student may request a full refund of all monies paid or apply all monies paid to the next scheduled class start date. The school reserves the right to change or modify the program contents, equipment, staff or materials as it deems necessary. Such changes may be necessary to keep pace with technological advances and to improve teaching methods or procedures. In no event will any such changes diminish the competency or content of any program or result in additional charges to the student.

While the school offers Placement Assistance, the school cannot, in any way, guarantee employment after the student has successfully completed the program of study.

The State of California established the Student Tuition Recovery Fund (STRF) to relieve or mitigate economic loss suffered by a student in an educational program at a qualifying institution, who is or was a California resident while enrolled, or was enrolled in a residency program, if the student enrolled in the institution, prepaid tuition, and suffered an economic loss. Unless relieved of the obligation to do so, you must pay the state-imposed assessment for the STRF, or it must be paid on your behalf, if you are a student in an educational program, who is a California resident, or are enrolled in a residency program, and prepay all or part of your tuition.

You are not eligible for protection from the STRF and you are not required to pay the STRF assessment, if you are not a California resident, or are not enrolled in a residency program.

Prior to signing this enrollment agreement, you must be given a catalog or brochure and a School Performance Fact Sheet, which you are encouraged to review prior to signing this agreement. These documents contain important policies and performance data for this institution. This institution is required to have you sign and date the information included in the School Performance Fact Sheet relating to completion rates, placement rates, license examination passage rates, salaries or wages, and the most recent three-year cohort default rate, if applicable, prior to signing this agreement.

I certify that I have received the catalog, School Performance Fact Sheet, and information regarding completion rates, placement rates, license examination passage rates, salary or wage information, and the most recent three-year cohort default rate, if applicable, included in the School Performance Fact sheet, and have signed, initialed, and dated the information provided in the School Performance Fact Sheet.

NOTICE CONCERNING TRANSFERABILITY OF CREDITS AND CREDENTIALS EARNED AT OUR INSTITUTION: The transferability of credits you earn at Brand College is at the complete discretion of an institution to which you may seek to transfer. Acceptance of the certificate you earn in the educational program is also at the complete discretion of the institution to which you may seek to transfer. If the certificates that you earn at this institution are not accepted at the institution to which you seek to transfer, you may be required to repeat some or all of your coursework at that institution. For this reason you should make certain that your

attendance at this institution will meet your educational goals. This may include contacting an institution to which you may seek to transfer after attending Brand College to determine if your certificate will transfer.

Academic Policies

Satisfactory Academic Progress - Description

The following is a description of the school's process and activities supporting a consistent SAP analysis and reporting on regular intervals.

1. Director of Education and the School Director meet during the Administrative Week following the conclusion of each school term.

2. The student transcripts are then sent to students via email. Official transcripts are sent to students per request.

3. Students who do not meet the required and satisfactory academic progress are placed on Probation I for one term.

4. Students who are on probation will be counseled by the school and a plan will be set to help the student to return to satisfactory standing with their academic progress. Students who are on probation are also on a limited enrollment plan. Full-time students can enroll for a maximum of 6 units while part-time students cannot take more than 3 units under this probationary period.

   Example of Satisfactory Academic Progress requirements (CCNP Program):

Program Interval	Satisfactory Completion	Minimum GPA
Module 1	25% or higher	1.0
Module 2	50% or higher	1.5
By completion of program	100%	2.0

5. If by the end of the first term in the probationary period the student meets the required and satisfactory academic progress, the student's status is then restored to satisfactory academic standing with the school.

6. In the event the student still does not meet the satisfactory academic progress at the end of the first probationary period, the student is then placed on Probation II and is suspended from the school for one term. While suspended, the student will go through counseling with the school in order to set a plan and return to satisfactory standing with the school.

7. At the end of the suspension period, the student has the option to submit a Petition for Reinstatement on Probationary Status form to provide information that may be deemed justifiable for the student's academic difficulties.

8. The school will review the information provided by the student and will determine if the student should be allowed to return to school based on the information provided by the student and verified by the school.

9. Should the school approve the student's return, the student will resume school under the status of Probation I as described above.

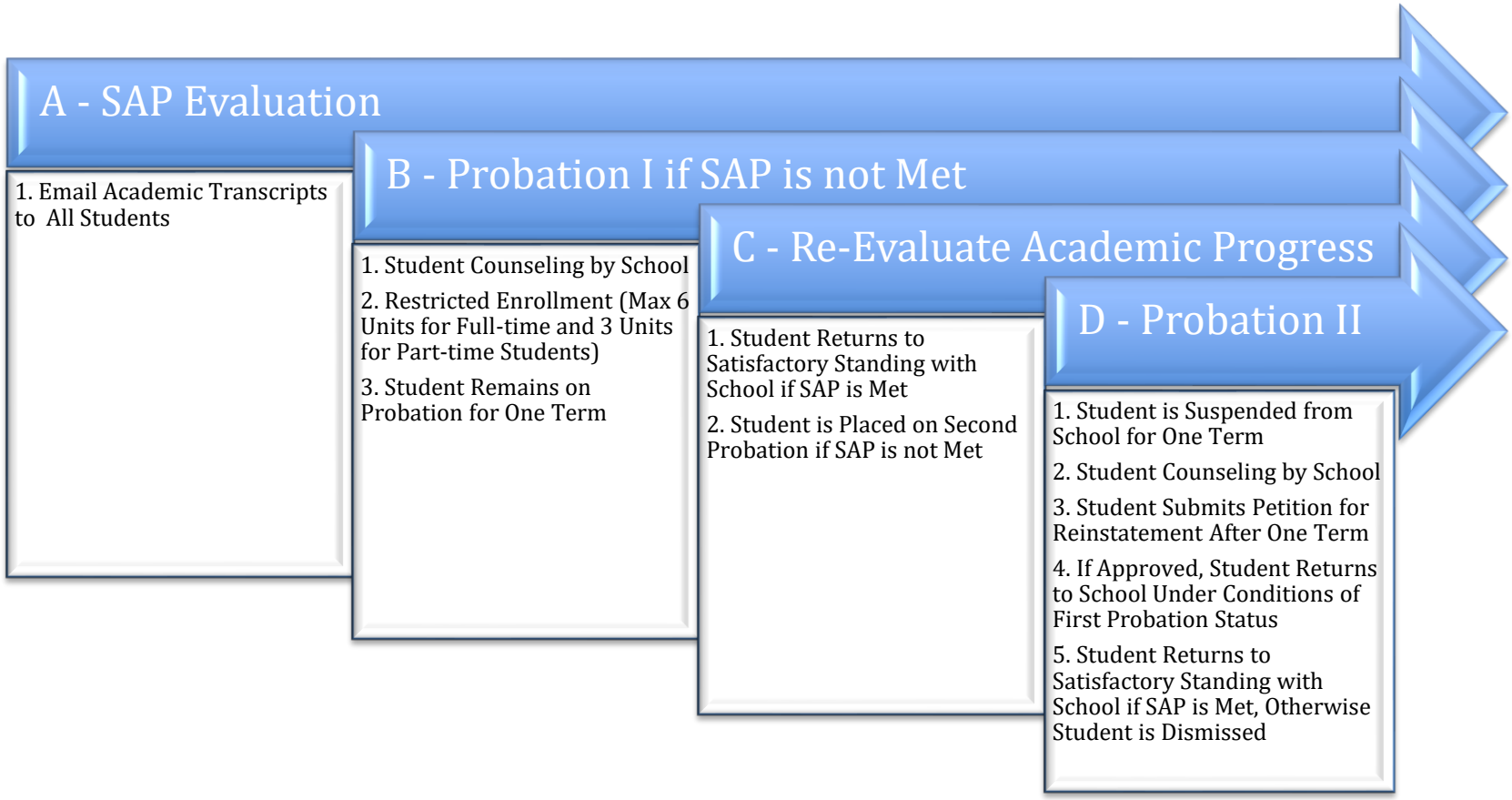
10. Upon the completion of the term, if the student meets the required and satisfactory academic progress, the student's status is then restored to satisfactory academic standing with the school.

The student is dismissed from the school otherwise. After six months, the student has the option to submit a petition for reinstatement.

The maximum time limit for a student to complete a program is 1.5 times the program length in weeks. If students do not complete the training within the maximum time frame they will be dropped from the program.

Program Name	Quarter (Clock Hours)	Length (in weeks)	Max Time (in weeks)
Cisco Certified Network Associate (CCNA)	96	12	18
Cisco Certified Network Professional (CCNP)	192	24	36
Cisco Certified Network Expert (CCNE)	624	78	117
Certified Network Technologies Expert (CNTE)	1152	72	108

Satisfactory Academic Progress – Process Flow



Attendance

A student in any class will be placed on attendance probation if she/he accumulates three consecutive or four cumulative unexcused absences. While on attendance probation, the student will be dismissed with an additional unexcused absence.

Tardiness

A student who is more than 15 minutes late to class, or who leave class more than one half hour early on four occasions will accrue one day of absence.

Make-Up Works

Students are required to make-up all assignments, exams, or other missed work as a result of an excused or unexcused absence. Arrangements to make up a missed exam must be made with the instructor.

Student Code of Conducts

To maintain an environment of social, moral and intellectual excellence, the college expects each student to behave in a mature and professional manner.

In essence, students need to display the following:

- Conduct that is orderly at all times
- Honesty & professionalism
- Respect for college and/or other student's property
- Professional attire
- Adhere to the requirements and guidelines provided in school's Virtual Training Guide document.
- Adhere to the requirements of Distance Learning Student Policy and Guide document

Disciplinary Dismissal

Any student who violates the following is liable for dismissal from her/his program:

- Student codes of conduct
- Cheating
- Drug/alcohol abuse
- Failure to meet financial obligations
- Failure to maintain satisfactory academic progress (SAP)
- Failure to comply with the School's policies (attendance, tardiness, etc.)

However, any student who has been dismissed may appeal the action, in writing, to the Director. The appeal must contain supporting, verifiable documentation that the unacceptable performance was the result of mitigating circumstances.

Conditions for Re-Enrollment

A student will be eligible for re-admissions if the director is satisfied with the evidence shown and the conditions that cause the interruption have been rectified.

Grading System

Grades are issued within two weeks after the end of each term. Designators indicate academic action, not grades, and are not included when computing academic averages. Grades and designators are assigned as follows:

Grade of F-Failing: A student, who receives an F in a required course, must repeat the course and receive a passing grade. Upon completion of a repeated course with a passing grade, the new grade will replace the failing grade in CGPA computation.

Index Grade	Percentage Equivalent	Grade Point
A	90-100	4
B	80-89	3
C	70-79	2
D	60-69	1
F	Below 60	0
I	Incomplete	0

Designators

P = Proficiency Test
T = Transfer Credit
W = Withdrawal

Grade of I-Incomplete: A grade of I signifies not all the required course work was completed during the term of enrollment. All required work must be completed by the end of the first week of the following term. If course requirements are not satisfied by the deadline, the grade I will be converted to an F.

Designator W-Course withdrawal: Designator W indicates that the student withdrew from a course prior to the withdrawal deadline. Students may withdraw from any program module from Monday of week 2 through Sunday of week 4 of the program. The student will receive a grade of "W" for any module the student drops. No adjustments will be made to tuition and fees for the quarter unless the student is withdrawing from all modules in the program. As soon as the student retakes and completes any dropped modules the new grade for the module will take effect in student's GPA and units will be added to the total units earned by the student.

Designator P-Proficiency test: Students may request a proficiency examination provided they have not previously taken the same class at Brand College.

Designator T-Transfer credit: An applicant wishing to transfer credit from another school must request a credit evaluation and provide an official transcript and a catalog from the transferring institution (grade must be 'C' or better). The Director will review the application and if the classes are determined to be equivalent to Brand College's curriculum, credits will be transferred. School credits are transferable only at the discretion of the receiving institution. Credits earned at Brand College may or may not transfer to other institutions.

Brand College does not offer Experiential learning credits.

Articulation Agreement: Brand College has not entered into an articulation or transfer agreement with any other college or university.

Student's Records

Brand College will be using specialized registrar software, which will organize the school's student population alphabetically and by social security number. The aforementioned software program is designed to also maintain data regarding students' personal information, attendance records, academic records and grades. A hard copy of each student's academic and financial records is kept in the school's administrative offices for 5 to 7 years. Academic and financial records are kept separately for the purpose of monitoring. Students transcripts are maintained permanently in Brand College's electronic database.

Student academic files contain the following items: student contract with school, personal data sheet, emergency medical form, entrance exam, and proof of most recent degree. (GED will be accepted in place of a high school diploma.

Complaint Policies and Procedure

Any individual with a complaint or a concern with the school is encouraged to reach out to the school faculty or staff members. There is a complaint log sheet available at the school's administrative desk. The complaint can be submitted either in writing or discussed verbally with the school faculty or staff. The recipient of the complaint shall report the complaint and any pertinent information to Debbie Ruiz (Academics) for further review and timely resolution. The complainant(s) will be kept informed as to the status of the complaint as well as the final resolution by the school.

Student Complaint Procedure

Schools accredited by the Accrediting Commission of Career Schools and Colleges must have a procedure and operational plan for handling student complaints. If a student does not feel that the school has adequately addressed a complaint or concern, the student may consider contacting the Accrediting

Commission. All complaints reviewed by the Commission must be in written form and should grant permission for the Commission to forward a copy of the complaint to the school for a response. This can be accomplished by filing the ACCSC Complaint Form. The complainant(s) will be kept informed as to the status of the complaint as well as the final resolution by the Commission.
Please direct all inquiries to:

Accrediting Commission of Career Schools and Colleges (ACCSC)
2101 Wilson Boulevard, Suite 302
Arlington, VA 22201
(703) 247-4212
www.accsc.org

A copy of the ACCSC Compliant Form is available at the school and may be obtained by contacting Debbie Ruiz, Director or online at www.accsc.org.

In addition to filing a complaint with the Accrediting Commission of Career Schools and Colleges (ACCSC), students may contact the Bureau of Private Postsecondary Education (BPPE). A student or any member of the public may file a complaint about this institution with the Bureau for Private Postsecondary Education by calling (888) 370-7589 or by completing a complaint form, which can be obtained on the bureau's internet website www.bppe.ca.gov.

Bureau of Private Postsecondary Education
P.O. Box 980818
West Sacramento, CA 95798
Tel: (888) 370-7589 or (916) 574-8900
Fax: (916) 263-1897
www.bppe.ca.gov

Graduation Requirements

A student must achieve a cumulative grade point average (CGPA) of at least 2.00 and satisfactorily complete all current curriculum requirements to graduate. Graduation will not be permitted if the best recorded grade of a required course is F, I or the designator W. Transfer credit and proficiency examination credit fulfill graduation requirements. A candidate who transferred to Brand College must complete at least 35 percent of the required credit hours at the school. Prior to receiving a certificate of completion, a student must satisfy all financial obligations to the school.

Brand College Services

Student Services

School will provide a number of vital services to students. Each student will be continually monitored and counseled as to the best course selection for his/her specific background and goals. These course goals will be re-evaluated each term, and altered if necessary. This will afford each student with a training program designed to fit his/her specific academic and personal needs. We believe that this flexibility will engender a higher rate of success for each student. Students who feel the need for extra work and instruction will be evaluated by an academic advisor and offered tutoring at no extra cost. School is dedicated to facilitating in the success of all students working to develop their computing skills and knowledge. For participating in distance education program, students will be continually monitored online or via virtual means such as by email, online chat, CMS, or online meeting using Google Meet.

Tutoring Assistance - Tutoring program is open to all students, at no cost. The program provides assistance on an individual basis or a group study when this format may be more appropriate. A tutor provides the tutoring with proficiency in the subject matter of the particular academic area. Tutoring is on an appointment basis. Students who wish to participate in the program or who are interested in becoming a tutor should contact the School Director. For participating in distance education, tutoring services are requested and scheduled via email. The tutoring session is conducted utilizing school's synchronous CMS or learning platform.

Learning Resources - The school library/resource center contains wide array of carefully selected resources to support the needs of the students, faculty and staff. The library/resource center has an extensive collection of books, magazines, journals, newspapers, and internet access to assist those pursuing our training programs and prepare those planning a career in the IT industry. The library/resource center is used to obtain in-depth information on the subject matter, prepare students for classroom discussions, and prepare students for the certification exams. Resources are assigned to provide students with access to course related material, including additional readings, review and lab answers, lab files, multimedia presentations, and course related web sites. For students enrolled in distance education programs; the school provides access to its online learning resource implemented utilizing Safari Books. Distance education students can request access by email and/or through school's asynchronous CMS on Google Classroom.

Assessment Assistance - Assessment tests are given to identify the student's skill level in English and Math. Test scores are evaluated and measured in reference to the prerequisites of pertaining training courses. The objective is to assist admissions representative in recommending the most appropriate courses to meet the students' skill level and educational goals. Students planning to enroll in distance education are expected to follow the same requirements and plan to complete the assessment requirements on campus.

Brand College delivers advanced level training in the Information Technology field. For both residential and distance education programs, all students are required to possess basic computer skills including the use of a personal computer with updated Windows operating system and a supported Internet browser. The required technical and computer skills assessment is conducted during the initial assessment process of the applicant by school's director and with the help of one of school's instructors as needed.

For distance education programs, students require access to a computer, supported Internet browser, and Internet service. The school will provide the required hardware and software as well as an Internet hotspot device should students need support with all or any parts of the required prerequisites.

The school director and instructor assigned to the distance education program conduct an orientation course with students to familiarize them with the tools the school utilizes as part of the distance education

program. The orientation course covers school's Course Management System (CMS) for asynchronous learning and Google Meet as its online video conferencing platform for synchronous instructions.

Academic Advising - Academic advising provides students with information about the requirements for the programs offered at the school. Students can obtain an academic plan that will include admission and general education requirements, as well as courses to best prepare them for their program of study. Distance education students request and obtain access to the academic plan by email and/or through school's asynchronous CMS on Google Classroom.

Placement Assistance - Placement assistance is free of charge and is provided for certified graduates. Certified graduates are referred to various companies and consulting firms in the network of schools contacts. The placement advisor will assist students in determining where their interests lie, where their strengths are and what work would provide a sense of fulfillment. Students will find assistance in investigating different career possibilities. For graduates from distance education programs, the school provides placement services and support online or via virtual means such as by email, online chat, or online meeting using Google Meet.

Testing Services - Brand College is authorized center for tests administrated by Pearson Vue. Students may take any Pearson Vue administrated exam in a professional and comfortable setting. Distance education students can contact school's test administrator to schedule their online exam.

Brand College does not have dormitory facilities under its control. Brand College does not offer student housing services and assumes no responsibility to find or assist a student in finding housing. According to Zillow.com, rentals in Glendale CA are approximately $1,400 month.

Placement Services

Placement assistance provides career information and referrals for part time and full-time employment, resume assistance, interview preparation, career planning, occupational information and academic counseling.

Organization's consulting wing has built a highly respected reputation in the computer industry, which will also greatly benefit students. School has established numerous contacts with various companies and consulting firms. This database of business contacts will be available to students, as well.

A staff member will be working (approximately 20 hours weekly) to develop and extend Brand College's relationship with various outlets. This staff member will also be working to place students on an as needed basis.

School will work diligently to establish a working relationship with the placement divisions of both Cisco Inc. and Microsoft Corporation - two industry giants. These affiliations will, undoubtedly, be very valuable resources for students involved in the network training programs.

While the school offers Placement Assistance, the school cannot, in any way; guarantee employment after the student has successfully completed the program of study.

Instructors

Name	Qualifications
Andre Abed	MCP, MCSE, MCT, MCTS, MCITP
Eduardo Argueta	MCSE, CCNA, CCNP
Alfons Manouk	MCP, MCSE, CCNA, CCNP
Thomas Kim	MCSE, CCNA, CCNP, CCSP
Jong Cho	CCNA, CCNP, CCSP

MCP Microsoft Certified Professional
MCSE Microsoft Certified Systems Engineer
MCT Microsoft Certified Trainer
MCTS Microsoft Certified Technology Specialist
MCITP Microsoft Certified IT Professional
CCNA Cisco Certified Network Associate
CCNP Cisco Certified Network Professional
CCSP Cisco Certified Security Professional

Academic Programs

The following academic programs are available for residential and distance education students.

Cisco Certified Network Associate (CCNA)

Program Summary

This instructor-led program with a combination of lecture and hands-on laboratory exercises validates the ability to install, configure, operate, and troubleshoot medium-size route and switched networks, including implementation and verification of connections to remote sites in a WAN. CCNA curriculum includes basic mitigation of security threats, introduction to wireless networking concepts and terminology, and performance-based skills. This new curriculum also includes (but is not limited to) the use of these protocols: IP, Enhanced Interior Gateway Routing Protocol (EIGRP), Serial Line Interface Protocol Frame Relay, Routing Information Protocol Version 2 (RIPv2), VLANs, Ethernet, access control lists (ACLs).

- Certification program
- 96 Contact Hours, 6 Credit Hours, 12 Weeks

Course No.	Course Name	Quarter Credit Hours	Clock Hours
CCA100	Administration I	6	96
	Total	**6**	**96**

Prerequisites

Candidates wishing to enter this course should have completed either a Microsoft or Linux+ networking program or have commensurate experience with PC networking and TCP/IP.

Type of Document Received Upon Graduation

Upon successful completion of all program requirements, each student will be awarded a Certificate of Completion.

Certification Tests

All certification exams are scored on a pass/fail basis. Depending on the specific exam, a correct response to 75% - 80% of the questions will be required to achieve a passing score. Students are encouraged to take exams immediately following completion of the corresponding course.

Career Development

Students who successfully complete this program will be prepared for entry to midlevel professional opportunities in the IT field with emphasis on installation, configuration and maintenance of Local Area Network (LAN) infrastructure. Although titles may vary by hiring organizations, students with these credentials are qualified to meet the requirements of positions such as Network Engineer, Network Support Specialist, Local Area Network Engineer, Network Systems Engineer or similar designations.

This program also aligns with the following career opportunities classified by US Department of Labor under the Standard Occupational Classification (SOC) system.

- 15-1142 Network and Computer System Administrators
- 15-1152 Computer Network Support Specialist

Recommended Next Course

Candidates wishing to further their education are recommended to consider the Cisco Certified Network Professional (CCNP) program as the next logical step towards becoming a well-rounded IT professional.

CCNA Program Details

COURSE CCA100

Title: Cisco Certified Network Associate
Exam: 200-301

Course Description
This instructor-led program with a combination of lecture and hands-on laboratory exercises covers basic networking concepts implemented on Cisco routers. Students will be introduced to the Cisco Internetworking Operating System (IOS) and its command structure. TCP/IP addressing and implementation, including subnetting, will be covered thoroughly. Wide Area Networking (WAN) implementations including ISDN, frame relay, and serial point-to-point (including T1), will be emphasized. This is an advanced course providing the skills and knowledge necessary to pass the Cisco certification exam (one exam) necessary to become a Cisco Certified Network Associate (CCNA).

Course Objectives
This course will cover the following subjects:

Part I - Introduction to Networking

Introduction to TCP/IP Networking
- Foundation Topics
- Perspectives on Networking
- TCP/IP Networking Model
- History Leading to TCP/IP
- Overview of the TCP/IP Networking Model
- TCP/IP Application Layer
- TCP/IP Transport Layer
- TCP/IP Network Layer
- TCP/IP Data-Link and Physical Layers
- Data Encapsulation Terminology
- Names of TCP/IP Messages
- OSI Networking Model and Terminology

Fundamentals of Ethernet LANs
- Foundation Topics
- An Overview of LANs
- Typical SOHO LANs
- Typical Enterprise LANs
- The Variety of Ethernet Physical Layer Standards
- Consistent Behavior over All Links Using the Ethernet Data-Link Layer
- Building Physical Ethernet LANs with UTP
- Transmitting Data Using Twisted Pairs
- Breaking Down a UTP Ethernet Link
- UTP Cabling Pinouts for 10BASE-T and 100BASE-T
- UTP Cabling Pinouts for 1000BASE-T
- Building Physical Ethernet LANs with Fiber
- Fiber Cabling Transmission Concepts
- Using Fiber with Ethernet
- Sending Data in Ethernet Networks
- Ethernet Data-Link Protocols
- Sending Ethernet Frames with Switches and Hubs

Fundamentals of WANs and IP Routing

- Foundation Topics
- Wide-Area Networks
- Leased-Line WANs
- Ethernet as a WAN Technology
- IP Routing
- Network Layer Routing (Forwarding) Logic
- How Network Layer Routing Uses LANs and WANs
- How IP Addressing Helps IP Routing
- How IP Routing Protocols Help IP Routing
- Other Network Layer Features
- Using Names and the Domain Name System
- The Address Resolution Protocol
- ICMP Echo and the ping Command

Part II - Implementing Ethernet LANs

Using the Command-Line Interface

- Foundation Topics
- Accessing the Cisco Catalyst Switch CLI
- Cisco Catalyst Switches
- Accessing the Cisco IOS CLI
- CLI Help Features
- The debug and show Commands
- Configuring Cisco IOS Software
- Configuration Submodes and Contexts
- Storing Switch Configuration Files
- Copying and Erasing Configuration Files

Analyzing Ethernet LAN Switching

- Foundation Topics
- LAN Switching Concepts
- Overview of Switching Logic
- Forwarding Known Unicast Frames
- Learning MAC Addresses
- Flooding Unknown Unicast and Broadcast Frames
- Avoiding Loops Using Spanning Tree Protocol
- LAN Switching Summary
- Verifying and Analyzing Ethernet Switching
- Demonstrating MAC Learning
- Switch Interfaces
- Finding Entries in the MAC Address Table
- Managing the MAC Address Table (Aging, Clearing)
- MAC Address Tables with Multiple Switches

Configuring Basic Switch Management

- Foundation Topics
- Securing the Switch CLI
- Securing User Mode and Privileged Mode with Simple Passwords
- Securing User Mode Access with Local Usernames and Passwords
- Securing User Mode Access with External Authentication Servers
- Securing Remote Access with Secure Shell
- Enabling IPv4 for Remote Access
- Host and Switch IP Settings
- Configuring IPv4 on a Switch
- Configuring a Switch to Learn Its IP Address with DHCP
- Verifying IPv4 on a Switch
- Miscellaneous Settings Useful in the Lab
- History Buffer Commands
- The logging synchronous, exec-timeout, and no ip domain-lookup Commands

Configuring and Verifying Switch Interfaces

- Foundation Topics
- Configuring Switch Interfaces
- Configuring Speed, Duplex, and Description
- Configuring Multiple Interfaces with the interface range Command
- Administratively Controlling Interface State with shutdown
- Removing Configuration with the no Command
- Autonegotiation
- Analyzing Switch Interface Status and Statistics
- Interface Status Codes and Reasons for Nonworking States
- Interface Speed and Duplex Issues
- Common Layer 1 Problems on Working Interfaces

Part III - Implementing VLANs and STP

Implementing Ethernet Virtual LANs

- Foundation Topics
- Virtual LAN Concepts
- Creating Multiswitch VLANs Using Trunking
- Forwarding Data Between VLANs
- VLAN and VLAN Trunking Configuration and Verification
- Creating VLANs and Assigning Access VLANs to an Interface
- VLAN Trunking Protocol
- VLAN Trunking Configuration
- Implementing Interfaces Connected to Phones
- Troubleshooting VLANs and VLAN Trunks
- Access VLANs Undefined or Disabled
- Mismatched Trunking Operational States
- The Supported VLAN List on Trunks
- Mismatched Native VLAN on a Trunk

Spanning Tree Protocol Concepts

- Foundation Topics
- STP and RSTP Basics
- The Need for Spanning Tree
- What Spanning Tree Does
- How Spanning Tree Works
- Configuring to Influence the STP Topology
- Details Specific to STP (and Not RSTP)
- STP Activity When the Network Remains Stable
- STP Timers That Manage STP Convergence
- Changing Interface States with STP
- Rapid STP Concepts
- Comparing STP and RSTP
- RSTP and the Alternate (Root) Port Role
- RSTP States and Processes
- RSTP and the Backup (Designated) Port Role
- RSTP Port Types
- Optional STP Features

RSTP and EtherChannel Configuration

- Foundation Topics
- Understanding RSTP Through Configuration
- The Need for Multiple Spanning Trees
- STP Modes and Standards
- The Bridge ID and System ID Extension
- How Switches Use the Priority and System ID Extension
- RSTP Methods to Support Multiple Spanning Trees
- Other RSTP Configuration Options
- Configuring Layer 2 EtherChannel
- Configuring a Manual Layer 2 EtherChannel
- Configuring Dynamic EtherChannels
- Physical Interface Configuration and EtherChannels
- EtherChannel Load Distribution

Part IV - IPv4 Addressing

Perspectives on IPv4 Subnetting

- Foundation Topics
- Introduction to Subnetting
- Subnetting Defined Through a Simple Example
- Operational View V.s. Design View of Subnetting
- Analyze Subnetting and Addressing Needs
- Rules about Which Hosts Are in Which Subnet
- Determining the Number of Subnets
- Determining the Number of Hosts per Subnet
- One Size Subnet Fits All–Or Not
- Make Design Choices
- Choose a Classful Network
- Choose the Mask
- Build a List of All Subnets
- Plan the Implementation
- Assigning Subnets to Different Locations

- *Choose Static and Dynamic Ranges per Subnet*

Analyzing Classful IPv4 Networks
- Foundation Topics
- Classful Network Concepts
- IPv4 Network Classes and Related Facts
- Number of Hosts per Network
- Deriving the Network ID and Related Numbers
- Unusual Network IDs and Network Broadcast Addresses
- Practice with Classful Networks
- Practice Deriving Key Facts Based on an IP Address
- Practice Remembering the Details of Address Classes

Analyzing Subnet Masks
- Foundation Topics
- Subnet Mask Conversion
- Three Mask Formats
- Converting Between Binary and Prefix Masks
- Converting Between Binary and DDN Masks
- Converting Between Prefix and DDN Masks
- Practice Converting Subnet Masks
- Identifying Subnet Design Choices Using Masks
- Masks Divide the Subnet's Addresses into Two Parts
- Masks and Class Divide Addresses into Three Parts
- Classless and Classful Addressing
- Calculations Based on the IPv4 Address Format
- Practice Analyzing Subnet Masks

Analyzing Existing Subnets
- Foundation Topics
- Defining a Subnet
- An Example with Network 172.16.0.0 and Four Subnets
- Subnet ID Concepts
- Subnet Broadcast Address
- Range of Usable Addresses
- Analyzing Existing Subnets: Binary
- Finding the Subnet ID: Binary
- Finding the Subnet Broadcast Address: Binary
- Binary Practice Problems
- Shortcut for the Binary Process
- Brief Note about Boolean Math
- Finding the Range of Addresses
- Analyzing Existing Subnets: Decimal
- Analysis with Easy Masks
- Predictability in the Interesting Octet
- Finding the Subnet ID: Difficult Masks
- Finding the Subnet Broadcast Address: Difficult Masks
- Practice Analyzing Existing Subnets
- A Choice: Memorize or Calculate

Part V - IPv4 Routing

Operating Cisco Routers
- Foundation Topics
- Installing Cisco Routers
- Installing Enterprise Routers
- Installing SOHO Routers
- Enabling IPv4 Support on Cisco Router Interfaces
- Accessing the Router CLI
- Router Interfaces
- Router Auxiliary Port

Configuring IPv4 Addresses and Static Routes
- Foundation Topics
- IP Routing
- IPv4 Routing Process Reference
- An Example of IP Routing
- Configuring IP Addresses and Connected Routes
- Connected Routes and the ip address Command
- The ARP Table on a Cisco Router
- Configuring Static Routes
- Static Network Routes
- Static Host Routes
- Floating Static Routes
- Static Default Routes
- Troubleshooting Static Routes
- IP Forwarding with the Longest Prefix Match
- Using show ip route to Find the Best Route
- Using show ip route address to Find the Best Route
- Interpreting the IP Routing Table

IP Routing in the LAN
- Foundation Topics
- VLAN Routing with Router 802.1Q Trunks
- Configuring ROAS
- Verifying ROAS
- Troubleshooting ROAS
- VLAN Routing with Layer 3 Switch SVIs
- Configuring Routing Using Switch SVIs
- Verifying Routing with SVIs
- Troubleshooting Routing with SVIs
- VLAN Routing with Layer 3 Switch Routed Ports
- Implementing Routed Interfaces on Switches
- Implementing Layer 3 EtherChannels
- Troubleshooting Layer 3 EtherChannels

Troubleshooting IPv4 Routing
- Foundation Topics
- Problem Isolation Using the ping Command
- Ping Command Basics
- Strategies and Results When Testing with the ping Command
- Using Ping with Names and with IP Addresses
- Problem Isolation Using the traceroute Command

- traceroute Basics
- Telnet and SSH
- Common Reasons to Use the IOS Telnet and SSH Client
- IOS Telnet and SSH Examples

Part VI - OSPF

Understanding OSPF Concepts
- Foundation Topics
- Comparing Dynamic Routing Protocol Features
- Routing Protocol Functions
- Interior and Exterior Routing Protocols
- Comparing IGPs
- Administrative Distance
- OSPF Concepts and Operation
- OSPF Overview
- Becoming OSPF Neighbors
- Exchanging the LSDB between Neighbors
- Calculating the Best Routes with SPF
- OSPF Areas and LSAs
- OSPF Areas
- How Areas Reduce SPF Calculation Time

Implementing OSPF
- Foundation Topics
- Implementing Single-Area OSPFv2
- OSPF Single-Area Configuration
- Wildcard Matching with the network Command
- Verifying OSPF Operation
- Verifying OSPF Configuration
- Configuring the OSPF Router ID
- Implementing Multiarea OSPF
- Using OSPFv2 Interface Subcommands
- OSPF Interface Configuration Example
- Additional OSPFv2 Features
- OSPF Passive Interfaces
- OSPF Default Routes
- OSPF Metrics (Cost)
- OSPF Load Balancing

OSPF Network Types and Neighbors
- Foundation Topics
- OSPF Network Types
- The OSPF Broadcast Network Type
- The OSPF Point-to-Point Network Type
- OSPF Neighbor Relationships
- OSPF Neighbor Requirements
- Issues That Prevent Neighbor Adjacencies
- Issues That Allow Adjacencies but Prevent IP Routes

Part VII - IP Version 6

Fundamentals of IP Version 6

- Foundation Topics
- Introduction to IPv6
- The Historical Reasons for IPv6
- The IPv6 Protocols
- IPv6 Routing
- IPv6 Routing Protocols
- IPv6 Addressing Formats and Conventions
- Representing Full (Unabbreviated) IPv6 Addresses
- Abbreviating and Expanding IPv6 Addresses
- Representing the Prefix Length of an Address
- Calculating the IPv6 Prefix (Subnet ID)
- Finding the IPv6 Prefix
- Working with More-Difficult IPv6 Prefix Lengths

IPv6 Addressing and Subnetting

- Foundation Topics
- Global Unicast Addressing Concepts
- Public and Private IPv6 Addresses
- The IPv6 Global Routing Prefix
- Address Ranges for Global Unicast Addresses
- IPv6 Subnetting Using Global Unicast Addresses
- Assigning Addresses to Hosts in a Subnet
- Unique Local Unicast Addresses
- Subnetting with Unique Local IPv6 Addresses
- The Need for Globally Unique Local Addresses

Implementing IPv6 Addressing on Routers

- Foundation Topics
- Implementing Unicast IPv6 Addresses on Routers
- Static Unicast Address Configuration
- Dynamic Unicast Address Configuration
- Special Addresses Used by Routers
- Link-Local Addresses
- IPv6 Multicast Addresses
- Miscellaneous IPv6 Addresses
- Anycast Addresses
- IPv6 Addressing Configuration Summary

Implementing IPv6 Routing

- Foundation Topics
- Connected and Local IPv6 Routes
- Rules for Connected and Local Routes
- Example of Connected IPv6 Routes
- Examples of Local IPv6 Routes
- Static IPv6 Routes
- Static Routes Using the Outgoing Interface
- Static Routes Using Next-Hop IPv6 Address
- Static Default Routes
- Static IPv6 Host Routes
- Floating Static IPv6 Routes

- Troubleshooting Static IPv6 Routes
- The Neighbor Discovery Protocol
- Discovering Neighbor Link Addresses with NDP NS and NA
- Discovering Routers with NDP RS and RA
- Using SLAAC with NDP RS and RA
- Discovering Duplicate Addresses Using NDP NS and NA
- NDP Summary

Part VIII - Wireless LANs

Fundamentals of Wireless Networks
- Foundation Topics
- Comparing Wired and Wireless Networks
- Wireless LAN Topologies
- Basic Service Set
- Distribution System
- Extended Service Set
- Independent Basic Service Set
- Other Wireless Topologies
- Repeater
- Workgroup Bridge
- Outdoor Bridge
- Mesh Network
- RF Overview
- Wireless Bands and Channels
- APs and Wireless Standards

Analyzing Cisco Wireless Architectures
- Foundation Topics
- Autonomous AP Architecture
- Cloud-based AP Architecture
- Split-MAC Architectures
- Comparing Wireless LAN Controller Deployments
- Cisco AP Modes

Securing Wireless Networks
- Foundation Topics
- Anatomy of a Secure Connection
- Authentication
- Message Privacy
- Message Integrity
- Wireless Client Authentication Methods
- Open Authentication
- WEP
- 802.1x/EAP
- Wireless Privacy and Integrity Methods
- TKIP
- CCMP
- GCMP
- WPA, WPA2, and WPA3

Building a Wireless LAN

- Foundation Topics
- Connecting a Cisco AP
- Accessing a Cisco WLC
- Connecting a Cisco WLC
- Using WLC Ports
- Using WLC Interfaces
- Configuring a WLAN:
- Configuring WLAN Security
- Configuring WLAN QoS
- Configuring Advanced WLAN Settings
- Finalizing WLAN Configuration

Cisco Certified Network Professional (CCNP)

Program Summary

This instructor-led program with a combination of lecture and hands-on laboratory exercises is designed to build advanced or journeyman knowledge of both LAN and WAN infrastructure implementations in a Cisco environment. This set of courses builds on the concepts introduced in the CCNA program. Students will be exposed to more in-depth concepts relating to routing implementation and design; TCP/IP design strategies; switching concepts; WAN optimization and performance issues; as well as, basic troubleshooting/support techniques and approaches. Some of the many protocols that will be studied include: TCP/IP, RIP, EIGRP, OSPF, IS-IS, BGP. Other topics include: VLAN implementation and management; spanning-tree protocol; multicast management; remote access implementation; Cisco security features including AAA; subnet concepts, design considerations, and implementation; VLSM; CIDR and more. These are advanced courses providing the skills and knowledge necessary to pass the Cisco certification exams (two exams) necessary to become a Cisco Certified Network Professional (CCNP).

- Certification program
- 192 Contact Hours, 12 Credit Hours, 24 Weeks

TERM 1

Course No.	Course Name	Quarter Credit Hours	Clock Hours
CCP100	Professional I	6	96
	Total	**6**	**96**

TERM 2

Course No.	Course Name	Quarter Credit Hours	Clock Hours
CCP110	Professional II	6	96
	Total	**6**	**96**

Prerequisites

Candidates wishing to enter this course should have completed the Cisco Certified Network Associate program or have commensurate experience WAN technologies in a Cisco environment.

Type of Document Received Upon Graduation

Upon successful completion of all program requirements, each student will be awarded a Certificate of Completion.

Certification Tests

All certification exams are scored on a pass/fail basis. Depending on the specific exam, a correct response to 75% - 80% of the questions will be required to achieve a passing score. Students are encouraged to take exams immediately following completion of the corresponding course.

Career Development
Students who successfully complete this program will be prepared for midlevel professional opportunities in the IT field with emphasis on design, installation, and configuration of Local Area Network (LAN) and Wide Area Network (WAN) infrastructure. Although titles may vary by hiring organizations, students with these credentials are qualified to meet the requirements of positions such as Sr. Network Engineer, Sr. Network Support Specialist, SR. WAN Engineer, Sr. LAN/WAN Engineer or similar designations.

This program also aligns with the following career opportunities classified by US Department of Labor under the Standard Occupational Classification (SOC) system.

- 15-1152 Computer Network Support Specialists
- 15-1143 Computer Network Architects
- 25-1021 Computer Science Teachers, Postsecondary

Recommended Next Course
Candidates wishing to further their education are recommended to consider the Cisco Certified Security Professional (CCNP Security) program as the next logical step towards becoming a well-rounded IT professional.

CCNP Program Details

COURSE CCP100

Title: Implementing Cisco Enterprise Advanced Routing and Services (ENARSI)
Exam: 350-401

Course Description
This instructor-led program with a combination of lecture and hands-on laboratory exercises will certify that the successful candidate has important knowledge and skills necessary to use advanced IP addressing and routing in implementing scalability for Cisco ISR routers connected to LANs and WANs. The Implementing and Operating Cisco Enterprise Network Core Technologies (ENCOR) v1.0 course gives students the knowledge and skills needed to configure, troubleshoot, and manage enterprise wired and wireless networks. Student will also learn to implement security principles within an enterprise network and how to overlay network design by using solutions such as SD-Access and SD-WAN. The exam covers topics on Advanced IP Addressing, Routing Principles, Multicast Routing, IPv6, Manipulating Routing Updates, Configuring basic BGP, Configuring EIGRP, OSPF, and IS-IS.

Course Objectives
This course will cover the following subjects:

- Illustrate the hierarchical network design model and architecture using the access, distribution, and core layers
- Compare and contrast the various hardware and software switching mechanisms and operation, while defining the Ternary Content Addressable Memory (TCAM) and Content Addressable Memory (CAM), along with process switching, fast switching, and Cisco Express Forwarding concepts
- Troubleshoot Layer 2 connectivity using VLANs and trunking
- Implementation of redundant switched networks using Spanning Tree Protocol
- Troubleshooting link aggregation using Etherchannel
- Describe the features, metrics, and path selection concepts of Enhanced Interior Gateway Routing Protocol (EIGRP)
- Implementation and optimization of Open Shortest Path First (OSPF)v2 and OSPFv3, including adjacencies, packet types, and areas, summarization, and route filtering for IPv4 and IPv6
- Implementing External Border Gateway Protocol (EBGP) interdomain routing, path selection, and single and dual-homed networking
- Implementing network redundancy using protocols including Hot Standby Routing Protocol (HSRP) and Virtual Router Redundancy Protocol (VRRP)
- Implementing internet connectivity within Enterprise using static and dynamic Network Address Translation (NAT)
- Describe the virtualization technology of servers, switches, and the various network devices and components
- Implementing overlay technologies such as Virtual Routing and Forwarding (VRF), Generic Routing Encapsulation (GRE), VPN, and Location Identifier Separation Protocol (LISP)
- Describe the components and concepts of wireless networking including Radio Frequency (RF) and antenna characteristics, and define the specific wireless standards
- Describe the various wireless deployment models available, include autonomous Access Point (AP) deployments and cloud-based designs within the centralized Cisco Wireless LAN Controller (WLC) architecture
- Describe wireless roaming and location services
- Describe how APs communicate with WLCs to obtain software, configurations, and centralized management

- Configure and verify Extensible Authentication Protocol (EAP), WebAuth, and Pre-shared Key (PSK) wireless client authentication on a WLC
- Troubleshoot wireless client connectivity issues using various available tools
- Troubleshooting Enterprise networks using services such as Network Time Protocol (NTP), Simple Network Management Protocol (SNMP), Cisco Internetwork Operating System (Cisco IOS®) IP Service Level Agreements (SLAs), NetFlow, and Cisco IOS Embedded Event Manager
- Explain the use of available network analysis and troubleshooting tools, which include show and debug commands, as well as best practices in troubleshooting
- Configure secure administrative access for Cisco IOS devices using the Command-Line Interface (CLI) access, Role-Based Access Control (RBAC), Access Control List (ACL), and Secure Shell (SSH), and explore device hardening concepts to secure devices from less secure applications, such as Telnet and HTTP
- Implement scalable administration using Authentication, Authorization, and Accounting (AAA) and the local database, while exploring the features and benefits
- Describe the enterprise network security architecture, including the purpose and function of VPNs, content security, logging, endpoint security, personal firewalls, and other security features
- Explain the purpose, function, features, and workflow of Cisco DNA Center™ Assurance for Intent-Based Networking, for network visibility, proactive monitoring, and application experience
- Describe the components and features of the Cisco SD-Access solution, including the nodes, fabric control plane, and data plane, while illustrating the purpose and function of the Virtual Extensible LAN (VXLAN) gateways
- Define the components and features of Cisco SD-WAN solutions, including the orchestration plane, management plane, control plane, and data plane
- Describe the concepts, purpose, and features of multicast protocols, including Internet Group Management Protocol (IGMP) v2/v3, Protocol-Independent Multicast (PIM) dense mode/sparse mode, and rendezvous points
- Describe the concepts and features of Quality of Service (QoS), and describe the need within the enterprise network
- Explain basic Python components and conditionals with script writing and analysis
- Describe network programmability protocols such as Network Configuration Protocol (NETCONF) and RESTCONF
- Describe APIs in Cisco DNA Center and vManage

COURSE CCP110

Title: Implementing Cisco Enterprise Advanced Routing and Services (ENARSI)
Exam: 300-410

Course Description

This instructor-led program with a combination of lecture and hands-on laboratory exercises will certify that the successful candidate has important knowledge and skills necessary to implement scalable multilayer networks. The Implementing Cisco Enterprise Advanced Routing and Services (ENARSI) v1.0 gives students the knowledge they need to install, configure, operate, and troubleshoot an enterprise network. This course covers advanced routing and infrastructure technologies, expanding on the topics covered in the Implementing and Operating Cisco Enterprise Network Core Technologies (ENCOR) v1.0 course. This course also will certify that the successful candidate has important knowledge and skills necessary to secure and expand the reach of an enterprise network to (1) plan and perform regular maintenance on complex enterprise routed and switched networks and (2) use technology-based practices and a systematic ITIL-compliant approach to perform network troubleshooting.

Course Objectives

This course will cover the following subjects:

- Configure classic Enhanced Interior Gateway Routing Protocol (EIGRP) and named EIGRP for IPv4 and IPv6
- Optimize classic EIGRP and named EIGRP for IPv4 and IPv6
- Troubleshoot classic EIGRP and named EIGRP for IPv4 and IPv6
- Configure Open Shortest Path First (OSPF)v2 and OSPFv3 in IPv4 and IPv6 environments
- Optimize OSPFv2 and OSPFv3 behavior
- Troubleshoot OSPFv2 for IPv4 and OSPFv3 for IPv4 and IPv6
- Implement route redistribution using filtering mechanisms
- Troubleshoot redistribution
- Implement path control using Policy-Based Routing (PBR) and IP service level agreement (SLA)
- Configure Multiprotocol-Border Gateway Protocol (MP-BGP) in IPv4 and IPv6 environments
- Optimize MP-BGP in IPv4 and IPv6 environments
- Troubleshoot MP-BGP for IPv4 and IPv6
- Describe the features of Multiprotocol Label Switching (MPLS)
- Describe the major architectural components of an MPLS VPN
- Identify the routing and packet forwarding functionalities for MPLS VPNs
- Explain how packets are forwarded in an MPLS VPN environment
- Implement Cisco Internetwork Operating System (IOS®) Dynamic Multipoint VPNs (DMVPNs)
- Implement Dynamic Host Configuration Protocol (DHCP)
- Describe the tools available to secure the IPV6 first hop
- Troubleshoot Cisco router security features
- Troubleshoot infrastructure security and services

Cisco Certified Network Expert (CCNE)

Program Summary
This instructor-led program with a combination of lecture and hands-on laboratory exercises covers networking concepts implemented on Cisco routers. Students will be introduced to the Cisco Internetworking Operating System (IOS) and its command structure. TCP/IP addressing and implementation, including subnetting, will be covered thoroughly. Wide Area Networking (WAN) implementations including ISDN, frame relay, and serial point-to-point (including T1), will be emphasized.

This program is also designed to build advanced or journeyman knowledge of both LAN and WAN infrastructure implementations in a Cisco environment. This set of courses builds on the concepts introduced in the CCNA program. Students will be exposed to more in-depth concepts relating to routing implementation and design; TCP/IP design strategies; switching concepts; WAN optimization and performance issues; as well as, basic troubleshooting/support techniques and approaches. Some of the many protocols that will be studied include: TCP/IP, RIP, EIGRP, OSPF, IS-IS, BGP. Other topics include: VLAN implementation and management; spanning-tree protocol; multicast management; remote access implementation; Cisco security features including AAA; subnet concepts, design considerations, and implementation; VLSM; CIDR and more.

In addition, this program covers advanced topics and concepts related to securing Cisco networks. This course covers a wide array of security topics including: Cisco IOS firewall implementation; PIX firewall technology and features; VPN concepts and implementation; IPSec; implementation and design of intrusion detection systems; Cisco's SAFE implementation; AAA; protocol monitoring and management and much more. The goal of this course is to give the student the tools and knowledge necessary to secure and manage complex network infrastructures – protecting data and productivity, as well as, reducing costs.

This program provides the skills and knowledge necessary to pass the Cisco certifications including Cisco Certified Network Associate (CCNA), Cisco Certified Network Professional (CCNP Route & Switch), and Cisco Certified Security Professional (CCNP Security).

- Certification program
- 624 Contact Hours, 39 Credit Hours, 78 Weeks

TERM 1

Course No.	Course Name	Quarter Credit Hours	Clock Hours
CCE100	Expert I	6	96
	Total	**6**	**96**

TERM 2

Course No.	Course Name	Quarter Credit Hours	Clock Hours
CCE110	Expert II	6	96
	Total	**6**	**96**

TERM 3

Course No.	Course Name	Quarter Credit Hours	Clock Hours
CCE120	Expert III	6	96
	Total	**6**	**96**

TERM 4

Course No.	Course Name	Quarter Credit Hours	Clock Hours
CCE130	Expert IV	3	48
CCE140	Expert V	3	48
	Total	**6**	**96**

TERM 5

Course No.	Course Name	Quarter Credit Hours	Clock Hours
CSP150	Expert VI	3	48
CCE160	Expert VII	3	48
	Total	**6**	**96**

TERM 6

Course No.	Course Name	Quarter Credit Hours	Clock Hours
CCE170	Expert VIII	3	48
CCE180	Expert IX	3	48
	Total	**6**	**96**

TERM 7

Course No.	Course Name	Quarter Credit Hours	Clock Hours
CCE190	Expert X	3	48
	Total	**3**	**48**

Prerequisites
Candidates wishing to enter this course should have completed either a Microsoft or Linux+ networking program or have commensurate experience with PC networking and TCP/IP.

Type of Document Received Upon Graduation
Upon successful completion of all program requirements, each student will be awarded a Certificate of Completion.

Certification Tests
All certification exams are scored on a pass/fail basis. Depending on the specific exam, a correct response to 75% - 80% of the questions will be required to achieve a passing score. Students are encouraged to take exams immediately following completion of the corresponding course.

Career Development

Students who successfully complete this program will be prepared for midlevel to advanced professional opportunities in the IT field with emphasis on installation, configuration and maintenance of Local Area Network (LAN) and Wide Area Network (WAN) infrastructure. Although titles may vary by hiring organizations, students with these credentials are qualified to meet the requirements of positions such as Sr. Network Design Engineer, Sr. Network Security Engineer, Sr. Network Design Specialist, Sr. Network Systems Manager, Network Support or similar designations.

This program also aligns with the following career opportunities classified by US Department of Labor under the Standard Occupational Classification (SOC) system.

- 15-1143 Computer Network Architects
- 25-1021 Computer Science Teacher, Postsecondary
- 11-3021 Computer & Information System Manager

CCNE Program Details

COURSE CCE100

Title: Cisco Certified Network Associate
Exam: 200-301

Course Description
This instructor-led program with a combination of lecture and hands-on laboratory exercises covers basic networking concepts implemented on Cisco routers. Students will be introduced to the Cisco Internetworking Operating System (IOS) and its command structure. TCP/IP addressing and implementation, including subnetting, will be covered thoroughly. Wide Area Networking (WAN) implementations including ISDN, frame relay, and serial point-to-point (including T1), will be emphasized. This is an advanced course providing the skills and knowledge necessary to pass the Cisco certification exam (one exam) necessary to become a Cisco Certified Network Associate (CCNA).

Course Objectives
This course will cover the following subjects:

Part I - Introduction to Networking

Introduction to TCP/IP Networking
- Foundation Topics
- Perspectives on Networking
- TCP/IP Networking Model
- History Leading to TCP/IP
- Overview of the TCP/IP Networking Model
- TCP/IP Application Layer
- TCP/IP Transport Layer
- TCP/IP Network Layer
- TCP/IP Data-Link and Physical Layers
- Data Encapsulation Terminology
- Names of TCP/IP Messages
- OSI Networking Model and Terminology

Fundamentals of Ethernet LANs
- Foundation Topics
- An Overview of LANs
- Typical SOHO LANs
- Typical Enterprise LANs
- The Variety of Ethernet Physical Layer Standards
- Consistent Behavior over All Links Using the Ethernet Data-Link Layer
- Building Physical Ethernet LANs with UTP
- Transmitting Data Using Twisted Pairs
- Breaking Down a UTP Ethernet Link
- UTP Cabling Pinouts for 10BASE-T and 100BASE-T
- UTP Cabling Pinouts for 1000BASE-T
- Building Physical Ethernet LANs with Fiber
- Fiber Cabling Transmission Concepts
- Using Fiber with Ethernet
- Sending Data in Ethernet Networks
- Ethernet Data-Link Protocols
- Sending Ethernet Frames with Switches and Hubs

Fundamentals of WANs and IP Routing

- Foundation Topics
- Wide-Area Networks
- Leased-Line WANs
- Ethernet as a WAN Technology
- IP Routing
- Network Layer Routing (Forwarding) Logic
- How Network Layer Routing Uses LANs and WANs
- How IP Addressing Helps IP Routing
- How IP Routing Protocols Help IP Routing
- Other Network Layer Features
- Using Names and the Domain Name System
- The Address Resolution Protocol
- ICMP Echo and the ping Command

Part II - Implementing Ethernet LANs

Using the Command-Line Interface

- Foundation Topics
- Accessing the Cisco Catalyst Switch CLI
- Cisco Catalyst Switches
- Accessing the Cisco IOS CLI
- CLI Help Features
- The debug and show Commands
- Configuring Cisco IOS Software
- Configuration Submodes and Contexts
- Storing Switch Configuration Files
- Copying and Erasing Configuration Files

Analyzing Ethernet LAN Switching

- Foundation Topics
- LAN Switching Concepts
- Overview of Switching Logic
- Forwarding Known Unicast Frames
- Learning MAC Addresses
- Flooding Unknown Unicast and Broadcast Frames
- Avoiding Loops Using Spanning Tree Protocol
- LAN Switching Summary
- Verifying and Analyzing Ethernet Switching
- Demonstrating MAC Learning
- Switch Interfaces
- Finding Entries in the MAC Address Table
- Managing the MAC Address Table (Aging, Clearing)
- MAC Address Tables with Multiple Switches

Configuring Basic Switch Management

- Foundation Topics
- Securing the Switch CLI
- Securing User Mode and Privileged Mode with Simple Passwords
- Securing User Mode Access with Local Usernames and Passwords
- Securing User Mode Access with External Authentication Servers
- Securing Remote Access with Secure Shell
- Enabling IPv4 for Remote Access
- Host and Switch IP Settings
- Configuring IPv4 on a Switch
- Configuring a Switch to Learn Its IP Address with DHCP
- Verifying IPv4 on a Switch
- Miscellaneous Settings Useful in the Lab
- History Buffer Commands
- The logging synchronous, exec-timeout, and no ip domain-lookup Commands

Configuring and Verifying Switch Interfaces

- Foundation Topics
- Configuring Switch Interfaces
- Configuring Speed, Duplex, and Description
- Configuring Multiple Interfaces with the interface range Command
- Administratively Controlling Interface State with shutdown
- Removing Configuration with the no Command
- Autonegotiation
- Analyzing Switch Interface Status and Statistics
- Interface Status Codes and Reasons for Nonworking States
- Interface Speed and Duplex Issues
- Common Layer 1 Problems on Working Interfaces

Part III - Implementing VLANs and STP

Implementing Ethernet Virtual LANs

- Foundation Topics
- Virtual LAN Concepts
- Creating Multiswitch VLANs Using Trunking
- Forwarding Data Between VLANs
- VLAN and VLAN Trunking Configuration and Verification
- Creating VLANs and Assigning Access VLANs to an Interface
- VLAN Trunking Protocol
- VLAN Trunking Configuration
- Implementing Interfaces Connected to Phones
- Troubleshooting VLANs and VLAN Trunks
- Access VLANs Undefined or Disabled
- Mismatched Trunking Operational States
- The Supported VLAN List on Trunks
- Mismatched Native VLAN on a Trunk

Spanning Tree Protocol Concepts

- Foundation Topics
- STP and RSTP Basics
- The Need for Spanning Tree
- What Spanning Tree Does
- How Spanning Tree Works
- Configuring to Influence the STP Topology
- Details Specific to STP (and Not RSTP)
- STP Activity When the Network Remains Stable
- STP Timers That Manage STP Convergence
- Changing Interface States with STP
- Rapid STP Concepts
- Comparing STP and RSTP
- RSTP and the Alternate (Root) Port Role
- RSTP States and Processes
- RSTP and the Backup (Designated) Port Role
- RSTP Port Types
- Optional STP Features

RSTP and EtherChannel Configuration

- Foundation Topics
- Understanding RSTP Through Configuration
- The Need for Multiple Spanning Trees
- STP Modes and Standards
- The Bridge ID and System ID Extension
- How Switches Use the Priority and System ID Extension
- RSTP Methods to Support Multiple Spanning Trees
- Other RSTP Configuration Options
- Configuring Layer 2 EtherChannel
- Configuring a Manual Layer 2 EtherChannel
- Configuring Dynamic EtherChannels
- Physical Interface Configuration and EtherChannels
- EtherChannel Load Distribution

Part IV - IPv4 Addressing

Perspectives on IPv4 Subnetting

- Foundation Topics
- Introduction to Subnetting
- Subnetting Defined Through a Simple Example
- Operational View V.s. Design View of Subnetting
- Analyze Subnetting and Addressing Needs
- Rules about Which Hosts Are in Which Subnet
- Determining the Number of Subnets
- Determining the Number of Hosts per Subnet
- One Size Subnet Fits All–Or Not
- Make Design Choices
- Choose a Classful Network
- Choose the Mask
- Build a List of All Subnets
- Plan the Implementation
- Assigning Subnets to Different Locations

- *Choose Static and Dynamic Ranges per Subnet*

Analyzing Classful IPv4 Networks
- Foundation Topics
- Classful Network Concepts
- IPv4 Network Classes and Related Facts
- Number of Hosts per Network
- Deriving the Network ID and Related Numbers
- Unusual Network IDs and Network Broadcast Addresses
- Practice with Classful Networks
- Practice Deriving Key Facts Based on an IP Address
- Practice Remembering the Details of Address Classes

Analyzing Subnet Masks
- Foundation Topics
- Subnet Mask Conversion
- Three Mask Formats
- Converting Between Binary and Prefix Masks
- Converting Between Binary and DDN Masks
- Converting Between Prefix and DDN Masks
- Practice Converting Subnet Masks
- Identifying Subnet Design Choices Using Masks
- Masks Divide the Subnet's Addresses into Two Parts
- Masks and Class Divide Addresses into Three Parts
- Classless and Classful Addressing
- Calculations Based on the IPv4 Address Format
- Practice Analyzing Subnet Masks

Analyzing Existing Subnets
- Foundation Topics
- Defining a Subnet
- An Example with Network 172.16.0.0 and Four Subnets
- Subnet ID Concepts
- Subnet Broadcast Address
- Range of Usable Addresses
- Analyzing Existing Subnets: Binary
- Finding the Subnet ID: Binary
- Finding the Subnet Broadcast Address: Binary
- Binary Practice Problems
- Shortcut for the Binary Process
- Brief Note about Boolean Math
- Finding the Range of Addresses
- Analyzing Existing Subnets: Decimal
- Analysis with Easy Masks
- Predictability in the Interesting Octet
- Finding the Subnet ID: Difficult Masks
- Finding the Subnet Broadcast Address: Difficult Masks
- Practice Analyzing Existing Subnets
- A Choice: Memorize or Calculate

Part V - IPv4 Routing

Operating Cisco Routers
- Foundation Topics
- Installing Cisco Routers
- Installing Enterprise Routers
- Installing SOHO Routers
- Enabling IPv4 Support on Cisco Router Interfaces
- Accessing the Router CLI
- Router Interfaces
- Router Auxiliary Port

Configuring IPv4 Addresses and Static Routes
- Foundation Topics
- IP Routing
- IPv4 Routing Process Reference
- An Example of IP Routing
- Configuring IP Addresses and Connected Routes
- Connected Routes and the ip address Command
- The ARP Table on a Cisco Router
- Configuring Static Routes
- Static Network Routes
- Static Host Routes
- Floating Static Routes
- Static Default Routes
- Troubleshooting Static Routes
- IP Forwarding with the Longest Prefix Match
- Using show ip route to Find the Best Route
- Using show ip route address to Find the Best Route
- Interpreting the IP Routing Table

IP Routing in the LAN
- Foundation Topics
- VLAN Routing with Router 802.1Q Trunks
- Configuring ROAS
- Verifying ROAS
- Troubleshooting ROAS
- VLAN Routing with Layer 3 Switch SVIs
- Configuring Routing Using Switch SVIs
- Verifying Routing with SVIs
- Troubleshooting Routing with SVIs
- VLAN Routing with Layer 3 Switch Routed Ports
- Implementing Routed Interfaces on Switches
- Implementing Layer 3 EtherChannels
- Troubleshooting Layer 3 EtherChannels

Troubleshooting IPv4 Routing
- Foundation Topics
- Problem Isolation Using the ping Command
- Ping Command Basics
- Strategies and Results When Testing with the ping Command
- Using Ping with Names and with IP Addresses
- Problem Isolation Using the traceroute Command

- traceroute Basics
- Telnet and SSH
- Common Reasons to Use the IOS Telnet and SSH Client
- IOS Telnet and SSH Examples

Part VI - OSPF

Understanding OSPF Concepts
- Foundation Topics
- Comparing Dynamic Routing Protocol Features
- Routing Protocol Functions
- Interior and Exterior Routing Protocols
- Comparing IGPs
- Administrative Distance
- OSPF Concepts and Operation
- OSPF Overview
- Becoming OSPF Neighbors
- Exchanging the LSDB between Neighbors
- Calculating the Best Routes with SPF
- OSPF Areas and LSAs
- OSPF Areas
- How Areas Reduce SPF Calculation Time

Implementing OSPF
- Foundation Topics
- Implementing Single-Area OSPFv2
- OSPF Single-Area Configuration
- Wildcard Matching with the network Command
- Verifying OSPF Operation
- Verifying OSPF Configuration
- Configuring the OSPF Router ID
- Implementing Multiarea OSPF
- Using OSPFv2 Interface Subcommands
- OSPF Interface Configuration Example
- Additional OSPFv2 Features
- OSPF Passive Interfaces
- OSPF Default Routes
- OSPF Metrics (Cost)
- OSPF Load Balancing

OSPF Network Types and Neighbors
- Foundation Topics
- OSPF Network Types
- The OSPF Broadcast Network Type
- The OSPF Point-to-Point Network Type
- OSPF Neighbor Relationships
- OSPF Neighbor Requirements
- Issues That Prevent Neighbor Adjacencies
- Issues That Allow Adjacencies but Prevent IP Routes

Part VII - IP Version 6

Fundamentals of IP Version 6

- Foundation Topics
- Introduction to IPv6
- The Historical Reasons for IPv6
- The IPv6 Protocols
- IPv6 Routing
- IPv6 Routing Protocols
- IPv6 Addressing Formats and Conventions
- Representing Full (Unabbreviated) IPv6 Addresses
- Abbreviating and Expanding IPv6 Addresses
- Representing the Prefix Length of an Address
- Calculating the IPv6 Prefix (Subnet ID)
- Finding the IPv6 Prefix
- Working with More-Difficult IPv6 Prefix Lengths

IPv6 Addressing and Subnetting

- Foundation Topics
- Global Unicast Addressing Concepts
- Public and Private IPv6 Addresses
- The IPv6 Global Routing Prefix
- Address Ranges for Global Unicast Addresses
- IPv6 Subnetting Using Global Unicast Addresses
- Assigning Addresses to Hosts in a Subnet
- Unique Local Unicast Addresses
- Subnetting with Unique Local IPv6 Addresses
- The Need for Globally Unique Local Addresses

Implementing IPv6 Addressing on Routers

- Foundation Topics
- Implementing Unicast IPv6 Addresses on Routers
- Static Unicast Address Configuration
- Dynamic Unicast Address Configuration
- Special Addresses Used by Routers
- Link-Local Addresses
- IPv6 Multicast Addresses
- Miscellaneous IPv6 Addresses
- Anycast Addresses
- IPv6 Addressing Configuration Summary

Implementing IPv6 Routing

- Foundation Topics
- Connected and Local IPv6 Routes
- Rules for Connected and Local Routes
- Example of Connected IPv6 Routes
- Examples of Local IPv6 Routes
- Static IPv6 Routes
- Static Routes Using the Outgoing Interface
- Static Routes Using Next-Hop IPv6 Address
- Static Default Routes
- Static IPv6 Host Routes
- Floating Static IPv6 Routes

- Troubleshooting Static IPv6 Routes
- The Neighbor Discovery Protocol
- Discovering Neighbor Link Addresses with NDP NS and NA
- Discovering Routers with NDP RS and RA
- Using SLAAC with NDP RS and RA
- Discovering Duplicate Addresses Using NDP NS and NA
- NDP Summary

Part VIII - Wireless LANs

Fundamentals of Wireless Networks
- Foundation Topics
- Comparing Wired and Wireless Networks
- Wireless LAN Topologies
- Basic Service Set
- Distribution System
- Extended Service Set
- Independent Basic Service Set
- Other Wireless Topologies
- Repeater
- Workgroup Bridge
- Outdoor Bridge
- Mesh Network
- RF Overview
- Wireless Bands and Channels
- APs and Wireless Standards

Analyzing Cisco Wireless Architectures
- Foundation Topics
- Autonomous AP Architecture
- Cloud-based AP Architecture
- Split-MAC Architectures
- Comparing Wireless LAN Controller Deployments
- Cisco AP Modes

Securing Wireless Networks
- Foundation Topics
- Anatomy of a Secure Connection
- Authentication
- Message Privacy
- Message Integrity
- Wireless Client Authentication Methods
- Open Authentication
- WEP
- 802.1x/EAP
- Wireless Privacy and Integrity Methods
- TKIP
- CCMP
- GCMP
- WPA, WPA2, and WPA3

Building a Wireless LAN

- Foundation Topics
- Connecting a Cisco AP
- Accessing a Cisco WLC
- Connecting a Cisco WLC
- Using WLC Ports
- Using WLC Interfaces
- Configuring a WLAN:
- Configuring WLAN Security
- Configuring WLAN QoS
- Configuring Advanced WLAN Settings
- Finalizing WLAN Configuration

COURSE CCE110

Title: Implementing Cisco Enterprise Advanced Routing and Services (ENARSI)
Exam: 350-401

Course Description

This instructor-led program with a combination of lecture and hands-on laboratory exercises will certify that the successful candidate has important knowledge and skills necessary to use advanced IP addressing and routing in implementing scalability for Cisco ISR routers connected to LANs and WANs. The Implementing and Operating Cisco Enterprise Network Core Technologies (ENCOR) v1.0 course gives students the knowledge and skills needed to configure, troubleshoot, and manage enterprise wired and wireless networks. Student will also learn to implement security principles within an enterprise network and how to overlay network design by using solutions such as SD-Access and SD-WAN. The exam covers topics on Advanced IP Addressing, Routing Principles, Multicast Routing, IPv6, Manipulating Routing Updates, Configuring basic BGP, Configuring EIGRP, OSPF, and IS-IS.

Course Objectives

This course will cover the following subjects:

- Illustrate the hierarchical network design model and architecture using the access, distribution, and core layers
- Compare and contrast the various hardware and software switching mechanisms and operation, while defining the Ternary Content Addressable Memory (TCAM) and Content Addressable Memory (CAM), along with process switching, fast switching, and Cisco Express Forwarding concepts
- Troubleshoot Layer 2 connectivity using VLANs and trunking
- Implementation of redundant switched networks using Spanning Tree Protocol
- Troubleshooting link aggregation using Etherchannel
- Describe the features, metrics, and path selection concepts of Enhanced Interior Gateway Routing Protocol (EIGRP)
- Implementation and optimization of Open Shortest Path First (OSPF)v2 and OSPFv3, including adjacencies, packet types, and areas, summarization, and route filtering for IPv4 and IPv6
- Implementing External Border Gateway Protocol (EBGP) interdomain routing, path selection, and single and dual-homed networking
- Implementing network redundancy using protocols including Hot Standby Routing Protocol (HSRP) and Virtual Router Redundancy Protocol (VRRP)
- Implementing internet connectivity within Enterprise using static and dynamic Network Address Translation (NAT)
- Describe the virtualization technology of servers, switches, and the various network devices and components
- Implementing overlay technologies such as Virtual Routing and Forwarding (VRF), Generic Routing Encapsulation (GRE), VPN, and Location Identifier Separation Protocol (LISP)
- Describe the components and concepts of wireless networking including Radio Frequency (RF) and antenna characteristics, and define the specific wireless standards
- Describe the various wireless deployment models available, include autonomous Access Point (AP) deployments and cloud-based designs within the centralized Cisco Wireless LAN Controller (WLC) architecture
- Describe wireless roaming and location services
- Describe how APs communicate with WLCs to obtain software, configurations, and centralized management
- Configure and verify Extensible Authentication Protocol (EAP), WebAuth, and Pre-shared Key (PSK) wireless client authentication on a WLC
- Troubleshoot wireless client connectivity issues using various available tools

- Troubleshooting Enterprise networks using services such as Network Time Protocol (NTP), Simple Network Management Protocol (SNMP), Cisco Internetwork Operating System (Cisco IOS®) IP Service Level Agreements (SLAs), NetFlow, and Cisco IOS Embedded Event Manager
- Explain the use of available network analysis and troubleshooting tools, which include show and debug commands, as well as best practices in troubleshooting
- Configure secure administrative access for Cisco IOS devices using the Command-Line Interface (CLI) access, Role-Based Access Control (RBAC), Access Control List (ACL), and Secure Shell (SSH), and explore device hardening concepts to secure devices from less secure applications, such as Telnet and HTTP
- Implement scalable administration using Authentication, Authorization, and Accounting (AAA) and the local database, while exploring the features and benefits
- Describe the enterprise network security architecture, including the purpose and function of VPNs, content security, logging, endpoint security, personal firewalls, and other security features
- Explain the purpose, function, features, and workflow of Cisco DNA Center™ Assurance for Intent-Based Networking, for network visibility, proactive monitoring, and application experience
- Describe the components and features of the Cisco SD-Access solution, including the nodes, fabric control plane, and data plane, while illustrating the purpose and function of the Virtual Extensible LAN (VXLAN) gateways
- Define the components and features of Cisco SD-WAN solutions, including the orchestration plane, management plane, control plane, and data plane
- Describe the concepts, purpose, and features of multicast protocols, including Internet Group Management Protocol (IGMP) v2/v3, Protocol-Independent Multicast (PIM) dense mode/sparse mode, and rendezvous points
- Describe the concepts and features of Quality of Service (QoS), and describe the need within the enterprise network
- Explain basic Python components and conditionals with script writing and analysis
- Describe network programmability protocols such as Network Configuration Protocol (NETCONF) and RESTCONF
- Describe APIs in Cisco DNA Center and vManage

COURSE CCE120

Title: Implementing Cisco Enterprise Advanced Routing and Services (ENARSI)
Exam: 300-410

Course Description

This instructor-led program with a combination of lecture and hands-on laboratory exercises will certify that the successful candidate has important knowledge and skills necessary to implement scalable multilayer networks. The Implementing Cisco Enterprise Advanced Routing and Services (ENARSI) v1.0 gives students the knowledge they need to install, configure, operate, and troubleshoot an enterprise network. This course covers advanced routing and infrastructure technologies, expanding on the topics covered in the Implementing and Operating Cisco Enterprise Network Core Technologies (ENCOR) v1.0 course. This course also will certify that the successful candidate has important knowledge and skills necessary to secure and expand the reach of an enterprise network to (1) plan and perform regular maintenance on complex enterprise routed and switched networks and (2) use technology-based practices and a systematic ITIL-compliant approach to perform network troubleshooting.

Course Objectives

This course will cover the following subjects:

- Configure classic Enhanced Interior Gateway Routing Protocol (EIGRP) and named EIGRP for IPv4 and IPv6
- Optimize classic EIGRP and named EIGRP for IPv4 and IPv6
- Troubleshoot classic EIGRP and named EIGRP for IPv4 and IPv6
- Configure Open Shortest Path First (OSPF)v2 and OSPFv3 in IPv4 and IPv6 environments
- Optimize OSPFv2 and OSPFv3 behavior
- Troubleshoot OSPFv2 for IPv4 and OSPFv3 for IPv4 and IPv6
- Implement route redistribution using filtering mechanisms
- Troubleshoot redistribution
- Implement path control using Policy-Based Routing (PBR) and IP service level agreement (SLA)
- Configure Multiprotocol-Border Gateway Protocol (MP-BGP) in IPv4 and IPv6 environments
- Optimize MP-BGP in IPv4 and IPv6 environments
- Troubleshoot MP-BGP for IPv4 and IPv6
- Describe the features of Multiprotocol Label Switching (MPLS)
- Describe the major architectural components of an MPLS VPN
- Identify the routing and packet forwarding functionalities for MPLS VPNs
- Explain how packets are forwarded in an MPLS VPN environment
- Implement Cisco Internetwork Operating System (IOS®) Dynamic Multipoint VPNs (DMVPNs)
- Implement Dynamic Host Configuration Protocol (DHCP)
- Describe the tools available to secure the IPV6 first hop
- Troubleshoot Cisco router security features
- Troubleshoot infrastructure security and services

COURSE CCE130

Title: Implementing and Operating Cisco Security Core Technologies (SCOR)
Exam: 350-701 SCOR

Course Description

The Implementing and Operating Cisco Security Core Technologies (SCOR) v1.0 course helps students prepare for the Cisco CCNP Security and CCIE Security certifications and for senior-level security roles. In this course, students will master the skills and technologies they need to implement core Cisco security solutions to provide advanced threat protection against cybersecurity attacks. Students will learn security for networks, cloud and content, endpoint protection, secure network access, visibility, and enforcements. They will get extensive hands-on experience deploying Cisco Firepower Next-Generation Firewall and Cisco Adaptive Security Appliance (ASA) Firewall; configuring access control policies, mail policies, and 802.1X Authentication; and more. You will get introductory practice on Cisco Stealthwatch Enterprise and Cisco Stealthwatch Cloud threat detection features.

Course Objectives

This course will cover the following subjects:

- Describing Information Security Concepts
- Information Security Overview
- Assets, Vulnerabilities, and Countermeasures
- Managing Risk
- Describing Common TCP/IP Attacks
- Legacy TCP/IP Vulnerabilities
- IP Vulnerabilities
- Internet Control Message Protocol (ICMP) Vulnerabilities
- Describing Common Network Application Attacks
- Password Attacks
- Domain Name System (DNS)-Based Attacks
- DNS Tunneling
- Describing Common Endpoint Attacks
- Buffer Overflow
- Malware
- Reconnaissance Attack
- Describing Network Security Technologies
- Defense-in-Depth Strategy
- Defending Across the Attack Continuum
- Network Segmentation and Virtualization Overview
- Deploying Cisco ASA Firewall
- Cisco ASA Deployment Types
- Cisco ASA Interface Security Levels
- Cisco ASA Objects and Object Groups
- Deploying Cisco Firepower Next-Generation Firewall
- Cisco Firepower NGFW Deployments
- Cisco Firepower NGFW Packet Processing and Policies
- Cisco Firepower NGFW Objects
- Deploying Email Content Security
- Cisco Email Content Security Overview
- Simple Mail Transfer Protocol (SMTP) Overview
- Email Pipeline Overview
- Deploying Web Content Security

- Cisco Web Security Appliance (WSA) Overview
- Deployment Options
- Network Users Authentication
- Deploying Cisco Umbrella
- Cisco Umbrella Architecture
- Deploying Cisco Umbrella
- Cisco Umbrella Roaming Client
- Explaining VPN Technologies and Cryptography
- VPN Definition
- VPN Types
- Secure Communication and Cryptographic Services
- Introducing Cisco Secure Site-to-Site VPN Solutions
- Site-to-Site VPN Topologies
- IPsec VPN Overview
- IPsec Static Crypto Maps
- Deploying Cisco IOS VTI-Based Point-to-Point IPsec VPNs
- Cisco IOS VTIs
- Static VTI Point-to-Point IPsec Internet Key Exchange (IKE) v2 VPN Configuration
- Deploying Point-to-Point IPsec VPNs on the Cisco ASA and Cisco Firepower NGFW
- Point-to-Point VPNs on the Cisco ASA and Cisco Firepower NGFW
- Cisco ASA Point-to-Point VPN Configuration
- Cisco Firepower NGFW Point-to-Point VPN Configuration
- Introducing Cisco Secure Remote Access VPN Solutions
- Remote Access VPN Components
- Remote Access VPN Technologies
- Secure Sockets Layer (SSL) Overview
- Deploying Remote Access SSL VPNs on the Cisco ASA and Cisco Firepower NGFW
- Remote Access Configuration Concepts
- Connection Profiles
- Group Policies
- Explaining Cisco Secure Network Access Solutions
- Cisco Secure Network Access
- Cisco Secure Network Access Components
- AAA Role in Cisco Secure Network Access Solution
- Describing 802.1X Authentication
- 802.1X and Extensible Authentication Protocol (EAP)
- EAP Methods
- Role of Remote Authentication Dial-in User Service (RADIUS) in 802.1X Communications
- Configuring 802.1X Authentication
- Cisco Catalyst® Switch 802.1X Configuration
- Cisco Wireless LAN Controller (WLC) 802.1X Configuration
- Cisco Identity Services Engine (ISE) 802.1X Configuration
- Describing Endpoint Security Technologies*
- Host-Based Personal Firewall
- Host-Based Anti-Virus
- Host-Based Intrusion Prevention System
- Deploying Cisco Advanced Malware Protection (AMP) for Endpoints
- Cisco AMP for Endpoints Architecture
- Cisco AMP for Endpoints Engines
- Retrospective Security with Cisco AMP
- Introducing Network Infrastructure Protection
- Identifying Network Device Planes
- Control Plane Security Controls

- Management Plane Security Controls
- Deploying Control Plane Security Controls
- Infrastructure ACLs
- Control Plane Policing
- Control Plane Protection
- Deploying Layer 2 Data Plane Security Controls
- Overview of Layer 2 Data Plane Security Controls
- Virtual LAN (VLAN)-Based Attacks Mitigation
- Spanning Tree Protocol (STP) Attacks Mitigation
- Deploying Layer 3 Data Plane Security Controls
- Infrastructure Antispoofing ACLs
- Unicast Reverse Path Forwarding
- IP Source Guard
- Deploying Management Plane Security Controls
- Cisco Secure Management Access
- Simple Network Management Protocol Version 3
- Secure Access to Cisco Devices
- Deploying Traffic Telemetry Methods
- Network Time Protocol
- Device and Network Events Logging and Export
- Network Traffic Monitoring Using NetFlow
- Deploying Cisco Stealthwatch Enterprise
- Cisco Stealthwatch Offerings Overview
- Cisco Stealthwatch Enterprise Required Components
- Flow Stitching and Deduplication
- Describing Cloud and Common Cloud Attacks
- Evolution of Cloud Computing
- Cloud Service Models
- Security Responsibilities in Cloud
- Securing the Cloud
- Cisco Threat-Centric Approach to Network Security
- Cloud Physical Environment Security
- Application and Workload Security
- Deploying Cisco Stealthwatch Cloud
- Cisco Stealthwatch Cloud for Public Cloud Monitoring
- Cisco Stealthwatch Cloud for Private Network Monitoring
- Cisco Stealthwatch Cloud Operations
- Describing Software-Defined Networking (SDN)
- Software-Defined Networking Concepts
- Network Programmability and Automation
- Cisco Platforms and APIs

COURSE CCE140

Title: Securing Networks with Cisco Firepower Next Generation Firewall (SSNGFW)
Exam: 300-710 SNCF

Course Description

The Securing Networks with Cisco Firepower Next Generation Firewall (SSNGFW) v1.0 course shows students how to deploy and use Cisco Firepower Threat Defense system. This hands-on course gives students knowledge and skills to use and configure Cisco Firepower Threat Defense technology, beginning with initial device setup and configuration and including routing, high availability, Cisco Adaptive Security Appliance (ASA) to Cisco Firepower Threat Defense migration, traffic control, and Network Address Translation (NAT). They will learn how to implement advanced Next-Generation Firewall (NGFW) and Next-Generation Intrusion Prevention System (NGIPS) features, including network intelligence, file type detection, network-based malware detection, and deep packet inspection. Students will also learn how to configure site-to-site VPN, remote-access VPN, and SSL decryption before moving on to detailed analysis, system administration, and troubleshooting.

Course Objectives

This course will cover the following subjects:

- Cisco Firepower Threat Defense Overview
- Cisco Firepower NGFW Device Configuration
- Cisco Firepower NGFW Traffic Control
- Cisco Firepower Discovery
- Implementing Access Control Policies
- Security Intelligence
- File Control and Advanced Malware Protection
- Next-Generation Intrusion Prevention Systems
- Network Analysis Policies
- Detailed Analysis Techniques
- Cisco Firepower Platform Integration
- Alerting and Correlation Policies
- Performing System Administration
- Firepower Troubleshooting
- Perform Initial Device Setup
- Perform Device Management
- Configure Network Discovery
- Implement an Access Control Policy
- Implement Security Intelligence
- Implement Control and Advanced Malware Protection
- Implement NGIPS
- Customize a Network Analysis Policy
- Perform Analysis
- Configure Firepower Platform Integration with Splunk
- Configure Alerting and Event Correlation
- Perform System Administration

COURSE CCE150

Title: Implementing and Configuring Cisco Identity Services Engine (SISE)
Exam: 300-715 SISE

Course Description

The Implementing and Configuring Cisco Identity Services Engine (SISE) v3.0 course shows students how to deploy and use Cisco Identity Services Engine (ISE) v2.4, an identity and access control policy platform that simplifies the delivery of consistent, highly secure access control across wired, wireless, and VPN connections. This hands-on course provides students with the knowledge and skills to implement and use Cisco ISE, including policy enforcement, profiling services, web authentication and guest access services, BYOD, endpoint compliance services, and TACACS+ device administration. Through expert instruction and hands-on practice, students will learn how to use Cisco ISE to gain visibility into what is happening in their network, streamline security policy management, and contribute to operational efficiency.

Course Objectives

This course will cover the following subjects:

- Introducing Cisco ISE Architecture and Deployment
- Using Cisco ISE as a Network Access Policy Engine
- Cisco ISE Use Cases
- Describing Cisco ISE Functions
- Cisco ISE Deployment Models
- Context Visibility
- Cisco ISE Policy Enforcement
- Using 802.1X for Wired and Wireless Access
- Using MAC Authentication Bypass for Wired and Wireless Access
- Introducing Identity Management
- Configuring Certificate Services
- Introducing Cisco ISE Policy
- Implementing Third-Party Network Access Device Support
- Introducing Cisco TrustSec
- Cisco TrustSec Configuration
- Easy Connect
- Web Authentication and Guest Services
- Introducing Web Access with Cisco ISE
- Introducing Guest Access Components
- Configuring Guest Access Settings
- Configuring Sponsor and Guest Portals
- Cisco ISE Profiler
- Introducing Cisco ISE Profiler
- Profiling Deployment and Best Practices
- Cisco ISE BYOD
- Introducing the Cisco ISE BYOD Process
- Describing BYOD Flow
- Configuring the My Devices Portal
- Configuring Certificates in BYOD Scenarios
- Cisco ISE Endpoint Compliance Services
- Introducing Endpoint Compliance Services
- Configuring Client Posture Services and Provisioning in Cisco ISE
- Working with Network Access Devices

- Review TACACS+
- Cisco ISE TACACS+ Device Administration
- Configure TACACS+ Device Administration
- TACACS+ Device Administration Guidelines and Best Practices
- Migrating from Cisco ACS to Cisco ISE

COURSE CCE160

Title: Securing Email with Cisco Email Security Appliance (SESA)
Exam: 300-720 SESA

Course Description

The Securing Email with Cisco Email Security Appliance (SESA) v3.1 course shows students how to deploy and use Cisco Email Security Appliance to establish protection for their email systems against phishing, business email compromise, and ransomware, and to help streamline email security policy management. This hands-on course provides students with the knowledge and skills to implement, troubleshoot, and administer Cisco Email Security Appliance, including key capabilities such as advanced malware protection, spam blocking, anti-virus protection, outbreak filtering, encryption, quarantines, and data loss prevention.

Couse Objectives

This course will cover the following subjects:

- Describing the Cisco Email Security Appliance
- Cisco Email Security Appliance Overview
- Technology Use Case
- Cisco Email Security Appliance Data Sheet
- SMTP Overview
- Email Pipeline Overview
- Installation Scenarios
- Initial Cisco Email Security Appliance Configuration
- Centralizing Services on a Cisco Content Security Management Appliance (SMA)
- Release Notes for AsyncOS 11.x
- Administering the Cisco Email Security Appliance
- Distributing Administrative Tasks
- System Administration
- Managing and Monitoring Using the Command Line Interface (CLI)
- Other Tasks in the GUI
- Advanced Network Configuration
- Using Email Security Monitor
- Tracking Messages
- Logging
- Controlling Sender and Recipient Domains
- Public and Private Listeners
- Configuring the Gateway to Receive Email
- Host Access Table Overview
- Recipient Access Table Overview
- Configuring Routing and Delivery Features
- Controlling Spam with Talos SenderBase and Anti-Spam
- SenderBase Overview
- Anti-Spam
- Managing Graymail
- Protecting Against Malicious or Undesirable URLs
- File Reputation Filtering and File Analysis
- Bounce Verification
- Using Anti-Virus and Outbreak Filters
- Anti-Virus Scanning Overview
- Sophos Anti-Virus Filtering
- McAfee Anti-Virus Filtering

- Configuring the Appliance to Scan for Viruses
- Outbreak Filters
- How the Outbreak Filters Feature Works
- Managing Outbreak Filters
- Using Mail Policies
- Email Security Manager Overview
- Mail Policies Overview
- Handling Incoming and Outgoing Messages Differently
- Matching Users to a Mail Policy
- Message Splintering
- Configuring Mail Policies
- Using Content Filters
- Content Filters Overview
- Content Filter Conditions
- Content Filter Actions
- Filter Messages Based on Content
- Text Resources Overview
- Using and Testing the Content Dictionaries Filter Rules
- Understanding Text Resources
- Text Resource Management
- Using Text Resources
- Using Message Filters to Enforce Email Policies
- Message Filters Overview
- Components of a Message Filter
- Message Filter Processing
- Message Filter Rules
- Message Filter Actions
- Attachment Scanning
- Examples of Attachment Scanning Message Filters
- Using the CLI to Manage Message Filters
- Message Filter Examples
- Configuring Scan Behavior
- Preventing Data Loss
- Overview of the Data Loss Prevention (DLP) Scanning Process
- Setting Up Data Loss Prevention
- Policies for Data Loss Prevention
- Message Actions
- Updating the DLP Engine and Content Matching Classifiers
- Using LDAP
- Overview of LDAP
- Working with LDAP
- Using LDAP Queries
- Authenticating End-Users of the Spam Quarantine
- Configuring External LDAP Authentication for Users
- Testing Servers and Queries
- Using LDAP for Directory Harvest Attack Prevention
- Spam Quarantine Alias Consolidation Queries
- Validating Recipients Using an SMTP Server
- SMTP Session Authentication
- Configuring AsyncOS for SMTP Authentication
- Authenticating SMTP Sessions Using Client Certificates
- Checking the Validity of a Client Certificate
- Authenticating User Using LDAP Directory

- Authenticating SMTP Connection Over Transport Layer Security (TLS) Using a Client Certificate
- Establishing a TLS Connection from the Appliance
- Updating a List of Revoked Certificates
- Email Authentication
- Email Authentication Overview
- Configuring DomainKeys and DomainKeys Identified Mail (DKIM) Signing
- Verifying Incoming Messages Using DKIM
- Overview of Sender Policy Framework (SPF) and SIDF Verification
- Domain-based Message Authentication Reporting and Conformance (DMARC) Verification
- Forged Email Detection
- Email Encryption
- Overview of Cisco Email Encryption
- Encrypting Messages
- Determining Which Messages to Encrypt
- Inserting Encryption Headers into Messages
- Encrypting Communication with Other Message Transfer Agents (MTAs)
- Working with Certificates
- Managing Lists of Certificate Authorities
- Enabling TLS on a Listener's Host Access Table (HAT)
- Enabling TLS and Certificate Verification on Delivery
- Secure/Multipurpose Internet Mail Extensions (S/MIME) Security Services
- Using System Quarantines and Delivery Methods
- Describing Quarantines
- Spam Quarantine
- Setting Up the Centralized Spam Quarantine
- Using Safelists and Blocklists to Control Email Delivery Based on Sender
- Configuring Spam Management Features for End Users
- Managing Messages in the Spam Quarantine
- Policy, Virus, and Outbreak Quarantines
- Managing Policy, Virus, and Outbreak Quarantines
- Working with Messages in Policy, Virus, or Outbreak Quarantines
- Delivery Methods
- Centralized Management Using Clusters
- Overview of Centralized Management Using Clusters
- Cluster Organization
- Creating and Joining a Cluster
- Managing Clusters
- Cluster Communication
- Loading a Configuration in Clustered Appliances
- Debugging Mail Flow Using Test Messages: Trace
- Using the Listener to Test the Appliance
- Troubleshooting the Network
- Troubleshooting the Listener
- Troubleshooting Email Delivery
- Troubleshooting Performance
- Web Interface Appearance and Rendering Issues
- Responding to Alerts
- Troubleshooting Hardware Issues
- Working with Technical Support
- Model Specifications for Large Enterprises
- Model Specifications for Midsize Enterprises and Small-to-Midsize Enterprises or Branch Offices
- Cisco Email Security Appliance Model Specifications for Virtual Appliances
- Packages and License

COURSE CCE170

Title: Securing the Web with Cisco Web Security Appliance (SWSA)
Exam: 300-725 SWSA

Course Description

The Securing the Web with Cisco Web Security Appliance (SWSA) v3.0 course shows students how to implement, use, and maintain Cisco® Web Security Appliance (WSA), powered by Cisco Talos, to provide advanced protection for business email and control against web security threats. Through a combination of expert instruction and hands-on practice, students will learn how to deploy proxy services, use authentication, implement policies to control HTTPS traffic and access, implement use control settings and policies, use the solution's anti-malware features, implement data security and data loss prevention, perform administration of Cisco WSA solution, and more.

Course Objectives

This course will cover the following subjects:

- Describing Cisco WSA
- Technology Use Case
- Cisco WSA Solution
- Cisco WSA Features
- Cisco WSA Architecture
- Proxy Service
- Integrated Layer 4 Traffic Monitor
- Data Loss Prevention
- Cisco Cognitive Intelligence
- Management Tools
- Cisco Advanced Web Security Reporting (AWSR) and Third-Party Integration
- Cisco Content Security Management Appliance (SMA)
- Deploying Proxy Services
- Explicit Forward Mode vs. Transparent Mode
- Transparent Mode Traffic Redirection
- Web Cache Control Protocol
- Web Cache Communication Protocol (WCCP) Upstream and Downstream Flow
- Proxy Bypass
- Proxy Caching
- Proxy Auto-Config (PAC) Files
- FTP Proxy
- Socket Secure (SOCKS) Proxy
- Proxy Access Log and HTTP Headers
- Customizing Error Notifications with End User Notification (EUN) Pages
- Utilizing Authentication
- Authentication Protocols
- Authentication Realms
- Tracking User Credentials
- Explicit (Forward) and Transparent Proxy Mode
- Bypassing Authentication with Problematic Agents
- Reporting and Authentication
- Re-Authentication
- FTP Proxy Authentication
- Troubleshooting Joining Domains and Test Authentication
- Integration with Cisco Identity Services Engine (ISE)

- Creating Decryption Policies to Control HTTPS Traffic
- Transport Layer Security (TLS)/Secure Sockets Layer (SSL) Inspection Overview
- Certificate Overview
- Overview of HTTPS Decryption Policies
- Activating HTTPS Proxy Function
- Access Control List (ACL) Tags for HTTPS Inspection
- Access Log Examples
- Understanding Differentiated Traffic Access Policies and Identification Profiles
- Overview of Access Policies
- Access Policy Groups
- Overview of Identification Profiles
- Identification Profiles and Authentication
- Access Policy and Identification Profiles Processing Order
- Other Policy Types
- Access Log Examples
- ACL Decision Tags and Policy Groups
- Enforcing Time-Based and Traffic Volume Acceptable Use Policies, and End User Notifications
- Defending Against Malware
- Web Reputation Filters
- Anti-Malware Scanning
- Scanning Outbound Traffic
- Anti-Malware and Reputation in Policies
- File Reputation Filtering and File Analysis
- Cisco Advanced Malware Protection
- File Reputation and Analysis Features
- Integration with Cisco Cognitive Intelligence
- Enforcing Acceptable Use Control Settings
- Controlling Web Usage
- URL Filtering
- URL Category Solutions
- Dynamic Content Analysis Engine
- Web Application Visibility and Control
- Enforcing Media Bandwidth Limits
- Software as a Service (SaaS) Access Control
- Filtering Adult Content
- Data Security and Data Loss Prevention
- Data Security
- Cisco Data Security Solution
- Data Security Policy Definitions
- Data Security Logs
- Performing Administration and Troubleshooting
- Monitor the Cisco Web Security Appliance
- Cisco WSA Reports
- Monitoring System Activity Through Logs
- System Administration Tasks
- Troubleshooting
- Command Line Interface
- References
- Comparing Cisco WSA Models
- Comparing Cisco SMA Models
- Overview of Connect, Install, and Configure
- Deploying the Cisco Web Security Appliance Open Virtualization Format (OVF) Template
- Mapping Cisco Web Security Appliance Virtual Machine (VM) Ports to Correct Networks

- Connecting to the Cisco Web Security Virtual Appliance
- Enabling Layer 4 Traffic Monitor (L4TM)
- Accessing and Running the System Setup Wizard
- Reconnecting to the Cisco Web Security Appliance
- High Availability Overview
- Hardware Redundancy
- Introducing Common Address Redundancy Protocol (CARP)
- Configuring Failover Groups for High Availability
- Feature Comparison Across Traffic Redirection Options
- Architecture Scenarios When Deploying Cisco AnyConnect Secure Mobility

COURSE CCE180

Title: Implementing Secure Solutions with Virtual Private Networks (SVPN)
Exam: 300-730 SVPN

Course Description

The Implementing Secure Solutions with Virtual Private Networks (SVPN) v1.0 course teaches students how to implement, configure, monitor, and support enterprise Virtual Private Network (VPN) solutions. Through a combination of lessons and hands-on experiences students will acquire the knowledge and skills to deploy and troubleshoot traditional Internet Protocol Security (IPsec), Dynamic Multipoint Virtual Private Network (DMVPN), FlexVPN, and remote access VPN to create secure and encrypted data, remote accessibility, and increased privacy.

Course Objectives

This course will cover the following subjects:

- Introducing VPN Technology Fundamentals
- Implementing Site-to-Site VPN Solutions
- Implementing Cisco Internetwork Operating System (Cisco IOS®) Site-to-Site FlexVPN Solutions
- Implement Cisco IOS Group Encrypted Transport (GET) VPN Solutions
- Implementing Cisco AnyConnect VPNs
- Implementing Clientless VPNs
- Explore IPsec Technologies
- Implement and Verify Cisco IOS Point-to-Point VPN
- Implement and Verify Cisco Adaptive Security Appliance (ASA) Point-to-Point VPN
- Implement and Verify Cisco IOS Virtual Tunnel Interface (VTI) VPN
- Implement and Verify Dynamic Multipoint VPN (DMVPN)
- Troubleshoot DMVPN
- Implement and Verify FlexVPN with Smart Defaults
- Implement and Verify Point-to-Point FlexVPN
- Implement and Verify Hub and Spoke FlexVPN
- Implement and Verify Spoke-to-Spoke FlexVPN
- Troubleshoot Cisco IOS FlexVPN
- Implement and Verify AnyConnect Transport Layer Security (TLS) VPN on ASA
- Implement and Verify Advanced Authentication, Authorization, and Accounting (AAA) on Cisco AnyConnect VPN
- Implement and Verify Clientless VPN on ASA

COURSE CCE190

Title: Implementing Automation for Cisco Security Solutions (SAUI)
Exam: 300-735 SAUTO

Course Description

The Implementing Automation for Cisco Security Solutions (SAUI) v1.0 course teaches students how to design advanced automated security solutions for their network. Through a combination of lessons and hands-on labs, they will master the use of modern programming concepts, RESTful Application Program Interfaces (APIs), data models, protocols, firewalls, web, Domain Name System (DNS), cloud, email security, and Cisco Identity Services Engine (ISE) to strengthen cybersecurity for their web services, network, and devices. Students will learn to work within the following platforms: Cisco Firepower Management Center, Cisco Firepower Threat Defense, Cisco ISE, Cisco pxGrid, Cisco Stealthwatch Enterprise, Cisco Stealthwatch Cloud, Cisco Umbrella, Cisco Advanced Malware Protection (AMP), Cisco Threat grid, and Cisco Security Management Appliances. This course will teach students when to use the API for each Cisco security solution to drive network efficiency and reduce complexity.

Course Objectives

This course will cover the following subjects:

- Introducing Cisco Security APIs
- Consuming Cisco Advanced Malware Protection APIs
- Using Cisco ISE
- Using Cisco pxGrid APIs
- Using Cisco Threat Grid APIs
- Investigating Cisco Umbrella Security Data Programmatically
- Exploring Cisco Umbrella Reporting and Enforcement APIs
- Automating Security with Cisco Firepower APIs
- Operationalizing Cisco Stealthwatch and the API Capabilities
- Using Cisco Stealthwatch Cloud APIs
- Describing Cisco Security Management Appliance APIs
- Query Cisco AMP Endpoint APIs for Verifying Compliance
- Use the REST API and Cisco pxGrid with Cisco Identity Services Engine
- Construct a Python Script Using the Cisco Threat Grid API
- Generate Reports Using the Cisco Umbrella Reporting API
- Explore the Cisco Firepower Management Center API
- Use Ansible to Automate Cisco Firepower Threat Defense Configuration
- Automate Firewall Policies Using the Cisco Firepower Device Manager API
- Automate Alarm Policies and Create Reports Using the Cisco Stealthwatch APIs
- Construct Reports Using Cisco Security Management Appliance (SMA) APIs

Certified Network Technologies Expert (CNTE)

Program Summary

This instructor-led program with a combination of lecture and hands-on laboratory exercises is our most comprehensive and diverse program combining the coursework of multiple disciplines. This program begins with a introductory class to fundamentals of networking which provides in-depth coursework basics of LAN and WAN environment and guides the student through multiple levels of network infrastructure study for Cisco, Juniper, Palo Alto, and other various environments. The goal of this program is to offer the student a single program to build the knowledge, skills, and certifications necessary to become a well-respected and well-trained professional poised to become a success in today's information technology environment.

- Certification program
- 1152 Contact Hours, 72 Credit Hours, 72 Weeks

TERM 1

Course No.	Course Name	Quarter Credit Hours	Clock Hours
CTE100	Technologies I	6	96
CTE110	Technologies II	6	96
	Total	**12**	**192**

TERM 2

Course No.	Course Name	Quarter Credit Hours	Clock Hours
CTE120	Technologies III	6	96
CTE130	Technologies IV	6	96
	Total	**12**	**192**

TERM 3

Course No.	Course Name	Quarter Credit Hours	Clock Hours
CTE140	Technologies V	6	96
CTE150	Technologies VI	6	96
	Total	**12**	**192**

TERM 4

Course No.	Course Name	Quarter Credit Hours	Clock Hours
CTE160	Technologies VII	6	96
CTE170	Technologies VIII	6	96
	Total	**12**	**192**

TERM 5

Course No.	Course Name	Quarter Credit Hours	Clock Hours
CTE180	Technologies IX	6	96
CTE190	Technologies X	6	96
	Total	**12**	**192**

TERM 6

Course No.	Course Name	Quarter Credit Hours	Clock Hours
CTE200	Technologies XI	6	96
CTE210	Technologies XII	6	96
	Total	**12**	**192**

Type of Document Received Upon Graduation
Upon successfully completing all requirements of the programs offered at Brand College, the student will be awarded a Certificate of Completion.

Certification Tests
Performance on a certification test is based on a pass or fail. You must receive between 75% and 80%, depending on the test, to pass. It is encouraged to take each test as soon as you complete the corresponding course.

Career Development
Students who successfully complete this program will be prepared for midlevel to advanced professional opportunities in the IT field with emphasis on installation, configuration and maintenance of Local Area Network (LAN) and Wide Area Network (WAN) infrastructure. In addition, the students are qualified for positions involving the planning, installation, and maintenance of client workstation as well as server operating system, applications and network infrastructure services using Microsoft and Linux technologies. Although titles may vary by hiring organizations, students with these credentials are qualified to meet the requirements of positions such as Sr. Network Design Engineer, Sr. Network Systems Manager, Manager of Network Systems or similar designations.

This program also aligns with the following career opportunities classified by US Department of Labor under the Standard Occupational Classification (SOC) system.

- 25-1021 Computer Science Teacher, Postsecondary
- 15-1152 Computer Network Support Specialist
- 15-1143 Computer Network Architects

CNTE Program Details

COURSE CTE100

Title: Network+ Certification
Exam: CompTIA Exam N10-008

Course Description
CompTIA Network+ covers the configuration, management, and troubleshooting of common wired and wireless network devices. Also included are emerging technologies such as unified communications, mobile, cloud, and virtualization technologies.

Course Objectives
This course will cover the following subjects:

Network Concepts
- Explain Purposes and Uses of Ports and Protocols
- Explain devices, applications, protocols and services at their appropriate OSI layers
- Explain the concepts and characteristics of routing and switching
- Given a scenario, configure the appropriate IP addressing components
- Compare and contrast the characteristics of network topologies, types and technologies
- Given a scenario, implement the appropriate wireless technologies and configurations
- Summarize cloud concepts and their purposes
- Explain the functions of network services

Infrastructure
- Given a scenario, deploy the appropriate cabling solution
- Given a scenario, determine the appropriate placement of networking devices on a network and install/configure them
- Explain the purposes and use cases for advanced networking devices
- Explain the purposes of virtualization and network storage technologies
- Compare and contrast WAN technologies

Network Operations
- Given a scenario, use appropriate documentation and diagrams to manage the network
- Compare and contrast business continuity and disaster recovery concepts
- Explain common scanning, monitoring and patching processes and summarize their expected outputs
- Given a scenario, use remote access methods
- Identify policies and best practices

Network Security
- Summarize the purposes of physical security devices
- Explain authentication and access controls
- Given a scenario, secure a basic wireless network
- Summarize common networking attacks
- Given a scenario, implement network device hardening
- Explain common mitigation techniques and their purposes

Network Troubleshooting and Tools

- Explain the network troubleshooting methodology
- Given a scenario, use the appropriate tool
- Given a scenario, troubleshoot common wired connectivity and performance issues
- Given a scenario, troubleshoot common wireless connectivity and performance issues
- Given a scenario, troubleshoot common network service issues

COURSE CTE110

Title: Cisco Certified Network Associate
Exam: 200-301

Course Description

This instructor-led program with a combination of lecture and hands-on laboratory exercises covers basic networking concepts implemented on Cisco routers. Students will be introduced to the Cisco Internetworking Operating System (IOS) and its command structure. TCP/IP addressing and implementation, including subnetting, will be covered thoroughly. Wide Area Networking (WAN) implementations including ISDN, frame relay, and serial point-to-point (including T1), will be emphasized. This is an advanced course providing the skills and knowledge necessary to pass the Cisco certification exam (one exam) necessary to become a Cisco Certified Network Associate (CCNA).

Course Objectives

This course will cover the following subjects:

Part I - Introduction to Networking

Introduction to TCP/IP Networking

- Foundation Topics
- Perspectives on Networking
- TCP/IP Networking Model
- History Leading to TCP/IP
- Overview of the TCP/IP Networking Model
- TCP/IP Application Layer
- TCP/IP Transport Layer
- TCP/IP Network Layer
- TCP/IP Data-Link and Physical Layers
- Data Encapsulation Terminology
- Names of TCP/IP Messages
- OSI Networking Model and Terminology

Fundamentals of Ethernet LANs

- Foundation Topics
- An Overview of LANs
- Typical SOHO LANs
- Typical Enterprise LANs
- The Variety of Ethernet Physical Layer Standards
- Consistent Behavior over All Links Using the Ethernet Data-Link Layer
- Building Physical Ethernet LANs with UTP
- Transmitting Data Using Twisted Pairs
- Breaking Down a UTP Ethernet Link
- UTP Cabling Pinouts for 10BASE-T and 100BASE-T
- UTP Cabling Pinouts for 1000BASE-T
- Building Physical Ethernet LANs with Fiber
- Fiber Cabling Transmission Concepts
- Using Fiber with Ethernet
- Sending Data in Ethernet Networks
- Ethernet Data-Link Protocols
- Sending Ethernet Frames with Switches and Hubs

Fundamentals of WANs and IP Routing

- Foundation Topics
- Wide-Area Networks
- Leased-Line WANs
- Ethernet as a WAN Technology
- IP Routing
- Network Layer Routing (Forwarding) Logic
- How Network Layer Routing Uses LANs and WANs
- How IP Addressing Helps IP Routing
- How IP Routing Protocols Help IP Routing
- Other Network Layer Features
- Using Names and the Domain Name System
- The Address Resolution Protocol
- ICMP Echo and the ping Command

Part II - Implementing Ethernet LANs

Using the Command-Line Interface

- Foundation Topics
- Accessing the Cisco Catalyst Switch CLI
- Cisco Catalyst Switches
- Accessing the Cisco IOS CLI
- CLI Help Features
- The debug and show Commands
- Configuring Cisco IOS Software
- Configuration Submodes and Contexts
- Storing Switch Configuration Files
- Copying and Erasing Configuration Files

Analyzing Ethernet LAN Switching

- Foundation Topics
- LAN Switching Concepts
- Overview of Switching Logic
- Forwarding Known Unicast Frames
- Learning MAC Addresses
- Flooding Unknown Unicast and Broadcast Frames
- Avoiding Loops Using Spanning Tree Protocol
- LAN Switching Summary
- Verifying and Analyzing Ethernet Switching
- Demonstrating MAC Learning
- Switch Interfaces
- Finding Entries in the MAC Address Table
- Managing the MAC Address Table (Aging, Clearing)
- MAC Address Tables with Multiple Switches

Configuring Basic Switch Management

- Foundation Topics
- Securing the Switch CLI
- Securing User Mode and Privileged Mode with Simple Passwords
- Securing User Mode Access with Local Usernames and Passwords
- Securing User Mode Access with External Authentication Servers
- Securing Remote Access with Secure Shell
- Enabling IPv4 for Remote Access
- Host and Switch IP Settings
- Configuring IPv4 on a Switch
- Configuring a Switch to Learn Its IP Address with DHCP
- Verifying IPv4 on a Switch
- Miscellaneous Settings Useful in the Lab
- History Buffer Commands
- The logging synchronous, exec-timeout, and no ip domain-lookup Commands

Configuring and Verifying Switch Interfaces

- Foundation Topics
- Configuring Switch Interfaces
- Configuring Speed, Duplex, and Description
- Configuring Multiple Interfaces with the interface range Command
- Administratively Controlling Interface State with shutdown
- Removing Configuration with the no Command
- Autonegotiation
- Analyzing Switch Interface Status and Statistics
- Interface Status Codes and Reasons for Nonworking States
- Interface Speed and Duplex Issues
- Common Layer 1 Problems on Working Interfaces

Part III - Implementing VLANs and STP

Implementing Ethernet Virtual LANs

- Foundation Topics
- Virtual LAN Concepts
- Creating Multiswitch VLANs Using Trunking
- Forwarding Data Between VLANs
- VLAN and VLAN Trunking Configuration and Verification
- Creating VLANs and Assigning Access VLANs to an Interface
- VLAN Trunking Protocol
- VLAN Trunking Configuration
- Implementing Interfaces Connected to Phones
- Troubleshooting VLANs and VLAN Trunks
- Access VLANs Undefined or Disabled
- Mismatched Trunking Operational States
- The Supported VLAN List on Trunks
- Mismatched Native VLAN on a Trunk

Spanning Tree Protocol Concepts

- Foundation Topics
- STP and RSTP Basics
- The Need for Spanning Tree
- What Spanning Tree Does
- How Spanning Tree Works
- Configuring to Influence the STP Topology
- Details Specific to STP (and Not RSTP)
- STP Activity When the Network Remains Stable
- STP Timers That Manage STP Convergence
- Changing Interface States with STP
- Rapid STP Concepts
- Comparing STP and RSTP
- RSTP and the Alternate (Root) Port Role
- RSTP States and Processes
- RSTP and the Backup (Designated) Port Role
- RSTP Port Types
- Optional STP Features

RSTP and EtherChannel Configuration

- Foundation Topics
- Understanding RSTP Through Configuration
- The Need for Multiple Spanning Trees
- STP Modes and Standards
- The Bridge ID and System ID Extension
- How Switches Use the Priority and System ID Extension
- RSTP Methods to Support Multiple Spanning Trees
- Other RSTP Configuration Options
- Configuring Layer 2 EtherChannel
- Configuring a Manual Layer 2 EtherChannel
- Configuring Dynamic EtherChannels
- Physical Interface Configuration and EtherChannels
- EtherChannel Load Distribution

Part IV - IPv4 Addressing

Perspectives on IPv4 Subnetting

- Foundation Topics
- Introduction to Subnetting
- Subnetting Defined Through a Simple Example
- Operational View V.s. Design View of Subnetting
- Analyze Subnetting and Addressing Needs
- Rules about Which Hosts Are in Which Subnet
- Determining the Number of Subnets
- Determining the Number of Hosts per Subnet
- One Size Subnet Fits All–Or Not
- Make Design Choices
- Choose a Classful Network
- Choose the Mask
- Build a List of All Subnets
- Plan the Implementation
- Assigning Subnets to Different Locations

- *Choose Static and Dynamic Ranges per Subnet*

Analyzing Classful IPv4 Networks
- Foundation Topics
- Classful Network Concepts
- IPv4 Network Classes and Related Facts
- Number of Hosts per Network
- Deriving the Network ID and Related Numbers
- Unusual Network IDs and Network Broadcast Addresses
- Practice with Classful Networks
- Practice Deriving Key Facts Based on an IP Address
- Practice Remembering the Details of Address Classes

Analyzing Subnet Masks
- Foundation Topics
- Subnet Mask Conversion
- Three Mask Formats
- Converting Between Binary and Prefix Masks
- Converting Between Binary and DDN Masks
- Converting Between Prefix and DDN Masks
- Practice Converting Subnet Masks
- Identifying Subnet Design Choices Using Masks
- Masks Divide the Subnet's Addresses into Two Parts
- Masks and Class Divide Addresses into Three Parts
- Classless and Classful Addressing
- Calculations Based on the IPv4 Address Format
- Practice Analyzing Subnet Masks

Analyzing Existing Subnets
- Foundation Topics
- Defining a Subnet
- An Example with Network 172.16.0.0 and Four Subnets
- Subnet ID Concepts
- Subnet Broadcast Address
- Range of Usable Addresses
- Analyzing Existing Subnets: Binary
- Finding the Subnet ID: Binary
- Finding the Subnet Broadcast Address: Binary
- Binary Practice Problems
- Shortcut for the Binary Process
- Brief Note about Boolean Math
- Finding the Range of Addresses
- Analyzing Existing Subnets: Decimal
- Analysis with Easy Masks
- Predictability in the Interesting Octet
- Finding the Subnet ID: Difficult Masks
- Finding the Subnet Broadcast Address: Difficult Masks
- Practice Analyzing Existing Subnets
- A Choice: Memorize or Calculate

Part V - IPv4 Routing

Operating Cisco Routers
- Foundation Topics
- Installing Cisco Routers
- Installing Enterprise Routers
- Installing SOHO Routers
- Enabling IPv4 Support on Cisco Router Interfaces
- Accessing the Router CLI
- Router Interfaces
- Router Auxiliary Port

Configuring IPv4 Addresses and Static Routes
- Foundation Topics
- IP Routing
- IPv4 Routing Process Reference
- An Example of IP Routing
- Configuring IP Addresses and Connected Routes
- Connected Routes and the ip address Command
- The ARP Table on a Cisco Router
- Configuring Static Routes
- Static Network Routes
- Static Host Routes
- Floating Static Routes
- Static Default Routes
- Troubleshooting Static Routes
- IP Forwarding with the Longest Prefix Match
- Using show ip route to Find the Best Route
- Using show ip route address to Find the Best Route
- Interpreting the IP Routing Table

IP Routing in the LAN
- Foundation Topics
- VLAN Routing with Router 802.1Q Trunks
- Configuring ROAS
- Verifying ROAS
- Troubleshooting ROAS
- VLAN Routing with Layer 3 Switch SVIs
- Configuring Routing Using Switch SVIs
- Verifying Routing with SVIs
- Troubleshooting Routing with SVIs
- VLAN Routing with Layer 3 Switch Routed Ports
- Implementing Routed Interfaces on Switches
- Implementing Layer 3 EtherChannels
- Troubleshooting Layer 3 EtherChannels

Troubleshooting IPv4 Routing
- Foundation Topics
- Problem Isolation Using the ping Command
- Ping Command Basics
- Strategies and Results When Testing with the ping Command
- Using Ping with Names and with IP Addresses
- Problem Isolation Using the traceroute Command

- traceroute Basics
- Telnet and SSH
- Common Reasons to Use the IOS Telnet and SSH Client
- IOS Telnet and SSH Examples

Part VI - OSPF

Understanding OSPF Concepts
- Foundation Topics
- Comparing Dynamic Routing Protocol Features
- Routing Protocol Functions
- Interior and Exterior Routing Protocols
- Comparing IGPs
- Administrative Distance
- OSPF Concepts and Operation
- OSPF Overview
- Becoming OSPF Neighbors
- Exchanging the LSDB between Neighbors
- Calculating the Best Routes with SPF
- OSPF Areas and LSAs
- OSPF Areas
- How Areas Reduce SPF Calculation Time

Implementing OSPF
- Foundation Topics
- Implementing Single-Area OSPFv2
- OSPF Single-Area Configuration
- Wildcard Matching with the network Command
- Verifying OSPF Operation
- Verifying OSPF Configuration
- Configuring the OSPF Router ID
- Implementing Multiarea OSPF
- Using OSPFv2 Interface Subcommands
- OSPF Interface Configuration Example
- Additional OSPFv2 Features
- OSPF Passive Interfaces
- OSPF Default Routes
- OSPF Metrics (Cost)
- OSPF Load Balancing

OSPF Network Types and Neighbors
- Foundation Topics
- OSPF Network Types
- The OSPF Broadcast Network Type
- The OSPF Point-to-Point Network Type
- OSPF Neighbor Relationships
- OSPF Neighbor Requirements
- Issues That Prevent Neighbor Adjacencies
- Issues That Allow Adjacencies but Prevent IP Routes

Part VII - IP Version 6

Fundamentals of IP Version 6

- Foundation Topics
- Introduction to IPv6
- The Historical Reasons for IPv6
- The IPv6 Protocols
- IPv6 Routing
- IPv6 Routing Protocols
- IPv6 Addressing Formats and Conventions
- Representing Full (Unabbreviated) IPv6 Addresses
- Abbreviating and Expanding IPv6 Addresses
- Representing the Prefix Length of an Address
- Calculating the IPv6 Prefix (Subnet ID)
- Finding the IPv6 Prefix
- Working with More-Difficult IPv6 Prefix Lengths

IPv6 Addressing and Subnetting

- Foundation Topics
- Global Unicast Addressing Concepts
- Public and Private IPv6 Addresses
- The IPv6 Global Routing Prefix
- Address Ranges for Global Unicast Addresses
- IPv6 Subnetting Using Global Unicast Addresses
- Assigning Addresses to Hosts in a Subnet
- Unique Local Unicast Addresses
- Subnetting with Unique Local IPv6 Addresses
- The Need for Globally Unique Local Addresses

Implementing IPv6 Addressing on Routers

- Foundation Topics
- Implementing Unicast IPv6 Addresses on Routers
- Static Unicast Address Configuration
- Dynamic Unicast Address Configuration
- Special Addresses Used by Routers
- Link-Local Addresses
- IPv6 Multicast Addresses
- Miscellaneous IPv6 Addresses
- Anycast Addresses
- IPv6 Addressing Configuration Summary

Implementing IPv6 Routing

- Foundation Topics
- Connected and Local IPv6 Routes
- Rules for Connected and Local Routes
- Example of Connected IPv6 Routes
- Examples of Local IPv6 Routes
- Static IPv6 Routes
- Static Routes Using the Outgoing Interface
- Static Routes Using Next-Hop IPv6 Address
- Static Default Routes
- Static IPv6 Host Routes
- Floating Static IPv6 Routes

- Troubleshooting Static IPv6 Routes
- The Neighbor Discovery Protocol
- Discovering Neighbor Link Addresses with NDP NS and NA
- Discovering Routers with NDP RS and RA
- Using SLAAC with NDP RS and RA
- Discovering Duplicate Addresses Using NDP NS and NA
- NDP Summary

Part VIII - Wireless LANs

Fundamentals of Wireless Networks
- Foundation Topics
- Comparing Wired and Wireless Networks
- Wireless LAN Topologies
- Basic Service Set
- Distribution System
- Extended Service Set
- Independent Basic Service Set
- Other Wireless Topologies
- Repeater
- Workgroup Bridge
- Outdoor Bridge
- Mesh Network
- RF Overview
- Wireless Bands and Channels
- APs and Wireless Standards

Analyzing Cisco Wireless Architectures
- Foundation Topics
- Autonomous AP Architecture
- Cloud-based AP Architecture
- Split-MAC Architectures
- Comparing Wireless LAN Controller Deployments
- Cisco AP Modes

Securing Wireless Networks
- Foundation Topics
- Anatomy of a Secure Connection
- Authentication
- Message Privacy
- Message Integrity
- Wireless Client Authentication Methods
- Open Authentication
- WEP
- 802.1x/EAP
- Wireless Privacy and Integrity Methods
- TKIP
- CCMP
- GCMP
- WPA, WPA2, and WPA3

Building a Wireless LAN

- Foundation Topics
- Connecting a Cisco AP
- Accessing a Cisco WLC
- Connecting a Cisco WLC
- Using WLC Ports
- Using WLC Interfaces
- Configuring a WLAN:
- Configuring WLAN Security
- Configuring WLAN QoS
- Configuring Advanced WLAN Settings
- Finalizing WLAN Configuration

COURSE CTE120

Title: Implementing Cisco Enterprise Advanced Routing and Services (ENARSI)
Exam: 350-401

Course Description

This instructor-led program with a combination of lecture and hands-on laboratory exercises will certify that the successful candidate has important knowledge and skills necessary to use advanced IP addressing and routing in implementing scalability for Cisco ISR routers connected to LANs and WANs. The Implementing and Operating Cisco Enterprise Network Core Technologies (ENCOR) v1.0 course gives students the knowledge and skills needed to configure, troubleshoot, and manage enterprise wired and wireless networks. Student will also learn to implement security principles within an enterprise network and how to overlay network design by using solutions such as SD-Access and SD-WAN. The exam covers topics on Advanced IP Addressing, Routing Principles, Multicast Routing, IPv6, Manipulating Routing Updates, Configuring basic BGP, Configuring EIGRP, OSPF, and IS-IS.

Course Objectives

This course will cover the following subjects:

- Illustrate the hierarchical network design model and architecture using the access, distribution, and core layers
- Compare and contrast the various hardware and software switching mechanisms and operation, while defining the Ternary Content Addressable Memory (TCAM) and Content Addressable Memory (CAM), along with process switching, fast switching, and Cisco Express Forwarding concepts
- Troubleshoot Layer 2 connectivity using VLANs and trunking
- Implementation of redundant switched networks using Spanning Tree Protocol
- Troubleshooting link aggregation using Etherchannel
- Describe the features, metrics, and path selection concepts of Enhanced Interior Gateway Routing Protocol (EIGRP)
- Implementation and optimization of Open Shortest Path First (OSPF)v2 and OSPFv3, including adjacencies, packet types, and areas, summarization, and route filtering for IPv4 and IPv6
- Implementing External Border Gateway Protocol (EBGP) interdomain routing, path selection, and single and dual-homed networking
- Implementing network redundancy using protocols including Hot Standby Routing Protocol (HSRP) and Virtual Router Redundancy Protocol (VRRP)
- Implementing internet connectivity within Enterprise using static and dynamic Network Address Translation (NAT)
- Describe the virtualization technology of servers, switches, and the various network devices and components
- Implementing overlay technologies such as Virtual Routing and Forwarding (VRF), Generic Routing Encapsulation (GRE), VPN, and Location Identifier Separation Protocol (LISP)
- Describe the components and concepts of wireless networking including Radio Frequency (RF) and antenna characteristics, and define the specific wireless standards
- Describe the various wireless deployment models available, include autonomous Access Point (AP) deployments and cloud-based designs within the centralized Cisco Wireless LAN Controller (WLC) architecture
- Describe wireless roaming and location services
- Describe how APs communicate with WLCs to obtain software, configurations, and centralized management
- Configure and verify Extensible Authentication Protocol (EAP), WebAuth, and Pre-shared Key (PSK) wireless client authentication on a WLC
- Troubleshoot wireless client connectivity issues using various available tools

- Troubleshooting Enterprise networks using services such as Network Time Protocol (NTP), Simple Network Management Protocol (SNMP), Cisco Internetwork Operating System (Cisco IOS®) IP Service Level Agreements (SLAs), NetFlow, and Cisco IOS Embedded Event Manager
- Explain the use of available network analysis and troubleshooting tools, which include show and debug commands, as well as best practices in troubleshooting
- Configure secure administrative access for Cisco IOS devices using the Command-Line Interface (CLI) access, Role-Based Access Control (RBAC), Access Control List (ACL), and Secure Shell (SSH), and explore device hardening concepts to secure devices from less secure applications, such as Telnet and HTTP
- Implement scalable administration using Authentication, Authorization, and Accounting (AAA) and the local database, while exploring the features and benefits
- Describe the enterprise network security architecture, including the purpose and function of VPNs, content security, logging, endpoint security, personal firewalls, and other security features
- Explain the purpose, function, features, and workflow of Cisco DNA Center™ Assurance for Intent-Based Networking, for network visibility, proactive monitoring, and application experience
- Describe the components and features of the Cisco SD-Access solution, including the nodes, fabric control plane, and data plane, while illustrating the purpose and function of the Virtual Extensible LAN (VXLAN) gateways
- Define the components and features of Cisco SD-WAN solutions, including the orchestration plane, management plane, control plane, and data plane
- Describe the concepts, purpose, and features of multicast protocols, including Internet Group Management Protocol (IGMP) v2/v3, Protocol-Independent Multicast (PIM) dense mode/sparse mode, and rendezvous points
- Describe the concepts and features of Quality of Service (QoS), and describe the need within the enterprise network
- Explain basic Python components and conditionals with script writing and analysis
- Describe network programmability protocols such as Network Configuration Protocol (NETCONF) and RESTCONF
- Describe APIs in Cisco DNA Center and vManage

COURSE CET130

Title: Implementing Cisco Enterprise Advanced Routing and Services (ENARSI)
Exam: 300-410

Course Description

This instructor-led program with a combination of lecture and hands-on laboratory exercises will certify that the successful candidate has important knowledge and skills necessary to implement scalable multilayer networks. The Implementing Cisco Enterprise Advanced Routing and Services (ENARSI) v1.0 gives students the knowledge they need to install, configure, operate, and troubleshoot an enterprise network. This course covers advanced routing and infrastructure technologies, expanding on the topics covered in the Implementing and Operating Cisco Enterprise Network Core Technologies (ENCOR) v1.0 course. This course also will certify that the successful candidate has important knowledge and skills necessary to secure and expand the reach of an enterprise network to (1) plan and perform regular maintenance on complex enterprise routed and switched networks and (2) use technology-based practices and a systematic ITIL-compliant approach to perform network troubleshooting.

Course Objectives

This course will cover the following subjects:

- Configure classic Enhanced Interior Gateway Routing Protocol (EIGRP) and named EIGRP for IPv4 and IPv6
- Optimize classic EIGRP and named EIGRP for IPv4 and IPv6
- Troubleshoot classic EIGRP and named EIGRP for IPv4 and IPv6
- Configure Open Shortest Path First (OSPF)v2 and OSPFv3 in IPv4 and IPv6 environments
- Optimize OSPFv2 and OSPFv3 behavior
- Troubleshoot OSPFv2 for IPv4 and OSPFv3 for IPv4 and IPv6
- Implement route redistribution using filtering mechanisms
- Troubleshoot redistribution
- Implement path control using Policy-Based Routing (PBR) and IP service level agreement (SLA)
- Configure Multiprotocol-Border Gateway Protocol (MP-BGP) in IPv4 and IPv6 environments
- Optimize MP-BGP in IPv4 and IPv6 environments
- Troubleshoot MP-BGP for IPv4 and IPv6
- Describe the features of Multiprotocol Label Switching (MPLS)
- Describe the major architectural components of an MPLS VPN
- Identify the routing and packet forwarding functionalities for MPLS VPNs
- Explain how packets are forwarded in an MPLS VPN environment
- Implement Cisco Internetwork Operating System (IOS®) Dynamic Multipoint VPNs (DMVPNs)
- Implement Dynamic Host Configuration Protocol (DHCP)
- Describe the tools available to secure the IPV6 first hop
- Troubleshoot Cisco router security features
- Troubleshoot infrastructure security and services

COURSE CTE140

Title: BGP

Course Description

BCG is the protocol which is used to make core routing decisions on the Internet; it involves a table of IP networks or "prefixes" which designate network reachability among autonomous systems (AS). BGP is a path vector protocol or a variant of a Distance-vector routing protocol. BGP does not involve traditional Interior Gateway Protocol (**IGP**) metrics, but routing decisions are made based on path, network policies and/or rule-sets. For this reason, it is more appropriately termed a reachability protocol rather than routing protocol. BGP was created to replace the Exterior Gateway Protocol (**EGP**) to allow fully decentralized routing in order to transition from the core ARPAnet model to a decentralized system that included the NSFNET backbone and its associated regional networks. This allowed the Internet to become a truly decentralized system.

Course Objectives

This course will cover the following subjects:

- Understanding BGP Building Blocks
- Comparing the Control Plane and Forwarding Plane.
- BGP Processes and Memory Use.
- BGP Path Attributes.
- Memory Use for IP CEF.
- Tuning BGP Performance
- TCP Protocol Considerations
- Path MTU Discovery, Queue Optimization
- Packet Reception Process. Hold Queue Optimization
- Effective BGP Policy Control
- How to Use Regular Expressions in Cisco IOS Software
- Filter Lists for Enforcing BGP Policies. Prefix Lists
- DESIGNING BGP ENTERPRISE NETWORKS
- Enterprise BGP Core Network Design
- Internet Connectivity for Enterprise Networks
- DESIGNING BGP SERVICE PROVIDER NETWORKS
- Scalable iBGP Design and Implementation Guidelines
- Route Reflection and Confederation Migration Strategies
- Service Provider Architecture
- General ISP Network Architecture
- Interior Gateway Protocol Layout
- The Aggregation Layer, Network Addressing Methodology, Loopback Addressing.
- IMPLEMENTING BGP MULTIPROTOCOL EXTENSIONS
- Multiprotocol BGP and MPLS VPN
- Route Distinguisher and VPN-IPv4 Address
- Understanding MPLS Fundamentals. MPLS Labels
- Multiprotocol BGP and Interdomain Multicast
- Multicast Distribution Trees
- Multiprotocol BGP Support for IPv
- IPv6 Enhancements, Expanded Addressing Capabilities, Autoconfiguration Capabilities
- MP-BGP Extensions for IPv6 NLRI, Dual-Stack Deployment, MP-BGP for IPv6 Deployment Considerations
- Configuring MP-BGP for IPv, BGP Address Family Configuration, Injecting IPv6 Prefixes into BGP
- Security Enhancements

- QoS Capabilities, IPv6 Addressing
- Anycast Address Functionality
- Aggregatable Global Unicast Addresses
- MP-BGP Extensions for IPv6 NLRI
- Multiprotocol BGP Extensions for CLNS Support
- Matrix of BGP Features and Cisco IOS Software Releases

COURSE CTE150

Title: MPLS

Course Description

MPLS is a highly scalable, protocol agnostic, data-carrying mechanism. In an MPLS network, data packets are assigned labels. Packet-forwarding decisions are made solely on the contents of this label, without the need to examine the packet itself. This allows one to create end-to-end circuits across any type of transport medium, using any protocol. The primary benefit is to eliminate dependence on a particular OSI model data link layer technology, such as Asynchronous (ATM), Frame Relay, Synchronous Optical Networking (SONET) or Ethernet, and eliminate the need for multiple layer-2 networks to satisfy different types of traffic. MPLS belongs to the family of packet-switched networks.

Course Objectives

This course will cover the following subjects:

- MPLS VPN Architecture Overview
- MPLS VPN Terminology
- Connection-Oriented VPNs
- Connectionless VPNs
- MPLS-Based VPNs
- New MPLS VPN Developments
- Advanced PE-CE Connectivity
- Remote Access to an MPLS VPN
- Providing Dial-In Access to an MPLS VPN
- Providing Dial-Out Access via LSDO
- Providing Dial-Out Backup for MPLS VPN Access
- Providing DSL Access to an MPLS VPN
- Advanced features of MPLS VPN Remote Access
- PE-CE Routing Protocol Enhancements and Advanced Features
- PE-CE Connectivity: OSPF
- PE-CE Connectivity: Integrated IS-IS
- PE-CE Connectivity: EIGRP
- Virtual Router Connectivity
- Configuring Virtual Routers on CE Routers
- VRF Selection based on Source IP Address
- Performing NAT in a Virtual Router Environment
- Protecting MPLS-VPN Backbone
- Inherent Security Capabilities
- Neighbor Authentication
- CE-to-CE Authentication
- PE to CE Circuits
- Large-Scale Routing and Multiple Service Provider Connectivity
- Carrier Backbone Connectivity
- Label Distribution Protocols on PE-CE Links
- BCP-4 Between PE/CE Routers
- Hierarchical VPNs: Carrier's Carrier MPLS VPNs
- Multicast VPN
- Introduction to IP Multicast
- Enterprise Multicast in a Service Provider Environment
- MDTs
- IP Version 6 Transport Across an MPLS Backbone

- IPv6 Business Drivers
- Deployment of IPv6 in Existing Networks
- 6PE Operation and Configuration
- Introduction to Troubleshooting of MPLS-Based Solutions
- MPLS Control Panel Troubleshooting
- MPLS Data Plane Troubleshooting

COURSE CTE160

Title: Implementing and Operating Cisco Service Provider Network Core Technologies (SPCOR)
Exam: 350-501

Course Description

The Implementing and Operating Cisco Service Provider Network Core Technologies (SPCOR) v1.0 course teaches students how to configure, verify, troubleshoot, and optimize next-generation, Service Provider IP network infrastructures. It provides a deep dive into Service Provider technologies including core architecture, services, networking, automation, quality of services, security, and network assurance.

Course Objectives

This course will cover the following subjects:

- Describing Service Provider Network Architectures
- Describing Cisco IOS Software Architectures
- Implementing OSPF
- Implementing IS-IS
- Implementing BGP
- Implementing Route Maps and Routing Protocol for LLN [Low-Power and Lossy Networks] (RPL)
- Transitioning to IPv6
- Implementing High Availability in Networking
- Implementing MPLS
- Implementing Cisco MPLS Traffic Engineering
- Describing Segment Routing
- Describing VPN Services
- Configuring L2VPN Services
- Configuring L3VPN Services
- Implementing Multicast
- Describing QoS Architecture
- Implementing QoS
- Implementing Control Plane Security
- Implementing Management Plane Security
- Implementing Data Plane Security
- Introducing Network Programmability
- Implementing Automation and Assurance
- Introducing Cisco NSO
- Implementing Virtualization in Service Provider Environments

COURSE CTE170

Title: Implementing Cisco service Provider Advanced Routing Solution (SPRI)
Exam: 350-510

Course Description

The Implementing Cisco Service Provider Advanced Routing Solutions (SPRI) course teaches students theories and practices to integrate advanced routing technologies including routing protocols, multicast routing, policy language, Multiprotocol Label Switching (MPLS), and segment routing, expanding their knowledge and skills in service provider core networks.

Course Objectives

This course will cover the following subjects:

- Implementing and Verifying Open Shortest Path First Multiarea Networks
- Implementing and Verifying Intermediate System to Intermediate System Multilevel Networks
- Introducing Routing Protocol Tools, Route Maps, and Routing Policy Language
- Implementing Route Redistribution
- Influencing Border Gateway Protocol Route Selection
- Scaling BGP in Service Provider Networks
- Securing BGP in Service Provider Networks
- Improving BGP Convergence and Implementing Advanced Operations
- Troubleshooting Routing Protocols
- Implementing and Verifying MPLS
- Implementing Cisco MPLS Traffic Engineering
- Implementing Segment Routing
- Describing Segment Routing Traffic Engineering (SR TE)
- Deploying IPv6 Tunneling Mechanisms
- Implementing IP Multicast Concepts and Technologies
- Implementing PIM-SM Protocol
- Implementing PIM-SM Enhancements
- Implementing Interdomain IP Multicast
- Implementing Distributed Rendezvous Point Solution in Multicast Network

COURSE CTE180

Title: Palo Alto Networks Certified Network Security Administrator
Test: PCNSA

Course Description

A Palo Alto Networks Certified Network Security Administrator (PCNSA) is capable of designing, deploying, configuring, maintaining and troubleshooting the vast majority of Palo Alto Networks-based network security implementations. Passing the PCNSA and exhibiting solid professional behavior, are the requirements for becoming a PCNSA. The formal certification exam is hosted and proctored by the third-party testing company Pearson VUE. Either exam should be taken by anyone who is prepared to demonstrate a deep understanding of Palo Alto Networks technologies. Candidates can be anyone who uses Palo Alto Networks products, including customers, partners, system engineers, systems integrators and support engineers.

Course Objectives

This course will cover the following subjects:

- Next-Generation Security Platform and Architecture
- Virtual and Cloud Deployment
- Initial Configuration
- Interface Configuration
- Security and NAT policies
- App-IDTM
- Content-IDTM
- URL Filtering
- Decryption
- WildFire
- User-IDTM
- GlobalProtectTM
- Site-to-Site VPNs
- Monitoring and Reporting
- Active/Passive High Availability
- Next-Generation Security Practices

COURSE CTE190

Title: Designing and Implementing Microsoft Azure Networking Solutions
Test: AZ-700

Course Description

This course teaches Network Engineers how to design, implement, and maintain Azure networking solutions. This course covers the process of designing, implementing, and managing core Azure networking infrastructure, Hybrid Networking connections, load balancing traffic, network routing, private access to Azure services, network security and monitoring. Learn how to design and implement a secure, reliable, network infrastructure in Azure and how to establish hybrid connectivity, routing, private access to Azure services, and monitoring in Azure.

Course Objectives

This course will cover the following subjects:

Introduction to Azure Virtual Networks

- Explore Azure Virtual Networks
- Configure public IP services
- Design name resolution for your Virtual Network
- Enable Cross-VNet connectivity with peering
- Implement virtual network traffic routing
- Configure internet access with Azure Virtual NAT

Design and Implement Hybrid Networking

- Design and implement Azure VPN Gateway
- Connect networks with Site-to-site VPN connections
- Connect devices to networks with Point-to-site VPN connections
- Connect remote resources by using Azure Virtual WANs
- Create a network virtual appliance (NVA) in a virtual hub

Design and Implement Azure ExpressRoute

- Explore Azure ExpressRoute
- Design an ExpressRoute deployment
- Configure peering for an ExpressRoute deployment
- Connect an ExpressRoute circuit to a VNet
- Connect geographically dispersed networks with ExpressRoute global reach
- Improve data path performance between networks with ExpressRoute FastPath
- Troubleshoot ExpressRoute connection issues

Load balance Non-HTTP(S) Traffic in Azure

- Explore load balancing
- Design and implement Azure load balancer using the Azure portal
- Explore Azure Traffic Manager

Load Balance HTTP(S) Traffic Azure

- Design Azure application gateway
- Configure Azure application gateway
- Design and configure Azure front door

Design and Implement Network Security

- Secure your virtual networks in the Azure portal
- Deploy Azure DDoS Protection by using the Azure portal
- Deploy Network Security Groups by using the Azure portal
- Design and implement Azure Firewall
- Working with Azure Firewall Manager
- Implement a Web Application Firewall on Azure Front Door

Design and Implement Private Access to Azure Services

- Explain virtual network service endpoints
- Define Private Link Service and private endpoint
- Integrate Private Link with DNS
- Integrate your App Service with Azure virtual networks

Design and Implement Network Monitoring

- Monitor your networks with Azure Monitor
- Monitor your networks with Azure Network Watcher

COURSE CTE200

Title: AWS Certified Advanced Networking - Specialty
Test: ANS-C00

Course Description

The course provides a level of expertise in advanced networking that significantly exceeds expectations of an AWS Certified Solutions Architect – Professional. The student is likely an experienced solutions architect who has a networking focus and who has design, implementation, and troubleshooting expertise. The candidate likely has a background in infrastructure engineering at scale (for example, complex SMB, enterprise, ISP, LAN/WAN environments). Recommended general IT knowledge The attendee should have knowledge in the following areas: Advanced networking architectures and interconnectivity options (for example, IP VPN, multiprotocol label switching [MPLS], virtual private LAN service [VPLS]), Networking technologies within the Open Systems Interconnection (OSI) model, and how they affect implementation decisions, Development of automation scripts and tools. Design, implementation, and optimization of the following: Routing architectures (including static and dynamic), Multi-Region solutions for a global enterprise, Highly available connectivity solutions (for example, AWS Direct Connect, VPN), CIDR and subnetting (IPv4 and IPv6), IPv6 transition challenges, and Generic solutions for network security features, including AWS WAF, intrusion detection systems (IDS), intrusion prevention systems (IPS), DDoS protection, and economic denial of service/sustainability (EDoS).

Course Objectives

This course will cover the following subjects:

Design and implement hybrid IT network architectures at scale

- VPC Subnets
- VPC CIDR Blocks
- VPC Subnets
- VPC Peering
- Flow Logs
- VPC Routing
- Routing Priorities
- Routing: VPC Peering
- Routing: Internet Gateways & NAT Gateways
- Routing: VPC Endpoints
- VPC IPsec VPNs

Design and implement AWS networks

- OSI and TCP/IP networking models
- Jumbo Frames

Automate AWS tasks

- Automation alternatives within AWS for network deployments
- Alternatives within AWS for network operations and management

Configure network integration with application services

- Evaluate DNS solutions in a hybrid IT architecture
- Leverage the capabilities of Route 53
- Determine the appropriate configuration of DHCP within AWS
- Determine a content-distribution strategy to optimize for performance using Amazon CloudFront

Design and implement for security and compliance

- Design requirements for alignment with security and compliance objectives
- Monitoring strategies in support of security and compliance objectives

Manage, optimize, and troubleshoot the network

- Tools and steps to troubleshoot and resolve network issues using hands-on labs and a preparation exam

COURSE CTE210

Title: VMware NSX-T Data Center: Install, Configure, Manage [V3.0]
Test: 2V0-41.20

Course Description

This in-depth class provides comprehensive training on how to install, configure, and manage a VMware NSX-T Data Center environment. This course covers key NSX-T Data Center features and functionality offered in the NSX-T Data Center 3.0 release, including the overall infrastructure, logical switching, logical routing, networking and security services, micro-segmentation and firewalls, and more.

Course Objectives

This course will cover the following subjects:

VMware Virtual Cloud Network and NSX-T Data Center

- Introduce VMware's Virtual Cloud Network vision
- Discuss NSX-T Data Center solutions, use cases, and benefits
- Explain NSX-T Data Center architecture and components
- Describe VMware NSX® product portfolio and features
- Explain the management, control, data, and consumption planes and function

Deployment Preparing the NSX-T Data Center Infrastructure

- Describe NSX Management Cluster
- Deploy VMware NSX® Manager™ nodes on VMware ESXi and KVM hypervisors
- Navigate through the NSX Manager UI
- Explain data-plane components such as N-VDS, transport nodes, transport zones, profiles, and more
- Perform transport node preparation and establish the data center infrastructure
- Verify transport node status and connectivity

NSX-T Data Center Logical Switching

- Introduce key components and terminology in logical switching
- Describe the function and types of L2 segments
- Explain tunneling and the GENEVE encapsulation
- Configure logical segments and attach hosts using NSX Manager UI
- Describe the function and types of segment profiles
- Create segment profiles and apply them to segments and ports
- Explain the function of MAC, ARP, and TEP tables used in packet forwarding
- Demonstrate L2 unicast packet flow
- Explain ARP suppression and BUM traffic handling

NSX-T Data Center Logical Routing

- Describe the logical routing function and use cases
- Introduce the two-tier routing architecture, topologies, and components
- Explain the Tier-0 and Tier-1 Gateway functions
- Describe the logical router components: Service Router and Distributed Router
- Discuss the architecture and function of VMware NSX® Edge™ nodes
- Discuss deployment options of NSX Edge nodes
- Configure NSX Edge nodes and create NSX Edge clusters
- Configure Tier-0 and Tier-1 Gateways
- Examine the single-tier and multitier packet flow
- Configure static routing and dynamic routing
- Enable ECMP on Tier-0 Gateway

- Describe NSX Edge HA, failure detection, and failback modes

NSX-T Data Center Bridging
- Describe the function of logical bridging
- Discuss the logical bridging use cases
- Compare routing and bridging solutions
- Explain the components of logical bridging
- Create bridge clusters and bridge profiles

NSX-T Data Center Security
- Introduce the NSX-T Data Center security approach and model
- Describe the micro-segmentation benefits and use cases
- Describe the Distributed Firewall architecture, components, and function
- Configure Distributed Firewall sections and rules
- Describe the Gateway Firewall architecture, components, and function
- Configure Gateway Firewall sections and rules
- Describe URL analysis and distributed intrusion system importance and use-cases.
- Describe the service insertion functionality for east-west and north-south security
- Discuss the integration and benefits of partner security solutions with NSX-T Data Center

NSX-T Data Center Services
- Describe NSX-T Data Center services
- Explain and configure Network Address Translation (NAT) and NAT 64
- Explain and configure DNS and DHCP services
- Describe the load-balancing function, topologies, components, and use cases
- Configure L4-L7 load balancing
- Discuss the IPSec VPN and L2 VPN function and use cases
- Configure IPSec VPN and L2 VPN using NSX Manager UI

NSX-T Data Center Monitoring
- Explain the importance and functionality of VMware NSX® Intelligence™
- Navigate through the NSX Topology UI and identify the various key elements in the UI
- Discuss the importance and use-cases of alarms and events

NSX-T Data Center User and Role Management
- Describe the function and benefits of VMware Identity Manager in NSX-T Data Center
- Integrate VMware Identity Manager with NSX-T Data Center
- Integrate LDAP with NSX-T Data Center
- Identify the various types of users, authentication policies, and permissions
- Use role-based access control to restrict user access
- Explain the built-in roles in VMware Identity Manager and role assignment to users

NSX-T Data Center Federation
- Introduce the NSX-T Data Center Federation key concepts, terminology, and use-cases
- Explain the onboarding process of NSX-T Data Center Federation
- Describe the NSX-T Data Center Federation switching and routing functions.
- Describe the NSX-T Data Center Federation security concepts and routing functions

2022 – 2023 Academic Calendar

Administrative Hours & Academic Hours:
All classes are online until further notice. Appointments are required for all campus visits.

2022 Winter Quarter:
Monday January 03 Term Begins
Sunday March 27 Term Ends
March 28 - April 03 Administrative Week (School Closed)

2022 Spring Quarter:
Monday April 04 Term Begins
Monday May 30 Memorial Day
Sunday June 26 Term Ends
June 27 - July 04 Administrative Week (School Closed)

2022 Summer Quarter:
Tuesday July 05 Term Begins
Monday September 05 Labor Day
Sunday September 25 Term Ends
September 26 - October 02 Administrative Week (School Closed)

2022 Fall Quarter:
Monday October 03 Term Begins
Thursday November 24 Thanksgiving
Saturday December 24 Term Ends
December 25 – January 01 Holidays (School Closed)

The school reserves the right to cancel a class due to insufficient enrollment.

2023 Winter Quarter:
Monday January 02 Term Begins
Sunday March 26 Term Ends
March 27 - April 02 Administrative Week (School Closed)

2023 Spring Quarter:
Monday April 03 Term Begins
Monday May 29 Memorial Day
Sunday June 25 Term Ends
June 26 - July 02 Administrative Week (School Closed)

2023 Summer Quarter:
Wednesday July 05 Term Begins
Sunday September 24 Term Ends
September 25 - October 01 Administrative Week (School Closed)

2023 Fall Quarter:
Monday October 02 Term Begins
Thursday November 23 Thanksgiving
Sunday December 24 Term Ends
December 25 – January 03 Holidays (School Closed)