T.C.
MİLLÎ EĞİTİM BAKANLIĞI
Talim ve Terbiye Kurulu Başkanlığı

SAYI: 53	**TARİH:** 04.06.2012	**KONU: CISCO (CCNP) Ağ Uzmanı Yetiştirme Kurs Programında Değişiklik Yapılması**
ÖNCEKİ KARARIN		
SAYI: 34	**TARİH:** 08.04.2011	

Özel Öğretim Kurumları Genel Müdürlüğünün 05.03.2012 tarihli ve 2077 sayılı teklif yazısı üzerine Kurulumuzda görüşülen **CISCO (CCNP) Ağ Uzmanı Yetiştirme Kurs Programı**nda ekli örneğine göre değişiklik yapılması kararlaştırıldı.

Ömer DİNÇER
Millî Eğitim Bakanı

Prof. Dr. Emin KARİP
Kurul Başkanı

(Görevli)
Dr. Hüseyin ŞİRİN
ÜYE

Prof. Dr. Mehmet BAYYİĞİT
ÜYE

Doç. Dr. Hatice DURAN YILDIZ
ÜYE

Abdülkadir YILMAZ
ÜYE

Prof. Dr. Cengiz ALACACI
ÜYE

İbrahim BÜKEL
ÜYE

Dr. İbrahim DEMİRCİ
ÜYE

T.C.
MİLLÎ EĞİTİM BAKANLIĞI
Talim ve Terbiye Kurulu Başkanlığı

CISCO (CCNP) AĞ UZMANI YETİŞTİRME KURS PROGRAMI

Ankara, 2012

KURUMUN ADI	**:**	
KURUMUN ADRESİ	**:**	
KURUCUSUNUN ADI	**:**	
PROGRAMIN ADI	**:**	"Cisco (CCNP) Ağ Uzmanı" Yetiştirme Kursu
PROGRAMIN DAYANAĞI	**:**	1739 sayılı Millî Eğitim Temel Kanunu, 3308 sayılı Meslekî Eğitim Kanunu, 5580 sayılı Özel Öğretim Kurumları Kanunu, Özel Öğretim Kurumları Yönetmeliği, Talim ve Terbiye Kurulu'nun 05.05.2005 tarih ve 24 sayılı "Özel Kurslar Çerçeve Programı"
PROGRAMIN SEVİYESİ	**:**	Program; en az ortaöğretim düzeyinde eğitimini tamamlamış kişiler için hazırlanmış olup kursiyerlerin, okuduğunu anlayacak düzeyde İngilizce bilgisine sahip olması gereklidir. Kurs programına, "Cisco (CCNA) Ağ Yöneticisi" kursunu tamamlamış veya eğitim kurumunca açılacak bu kursa ait "düzey belirleme" sınavından 90 ve üzeri not almış olan kişiler katılabilir.

PROGRAMIN AMAÇLARI

Bu program ile kursiyerlerin;

1. Ağ teknolojileri konusunda ileri düzeyde bilgi birikimi oluşturmaları,
2. Gelişmiş ağ protokollerini tanımaları ve planlayabilmeleri,
3. Ağda yedekleme teknolojilerini kavrayarak yedekleme yapabilme becerisi kazanmaları,
4. Ağdaki hataları bulup giderme becerisi kazanmaları,
5. Cisco cihazlarını kullanarak küçük ve orta ölçekli networkler kurabilmeleri

beklenmektedir.

PROGRAMIN UYGULANMASIYLA İLGİLİ AÇIKLAMALAR

1. Günümüzde, özel ve kamuda mevcut her türlü elektronik haberleşme ağlarının kurulup yönetilebilmesi için yeterli bilgi ve beceriye sahip değişik seviyede uzmanlık derecelerinde (yönetici düzeyi, uzman düzeyi, danışman düzeyi vb.) elemanlara ihtiyaç vardır. Ayrıca elektronik güvenlik sistemleri, akıllı bina ve fabrika otomasyon cihazlarının haberleşmesi gibi konularda yetişmiş insan gücü açığı mevcuttur ve bu açık giderek artmaktadır. Bu kurs programı ile kursiyerlere, orta düzeyde (uzman düzeyi) ihtiyaç duyulan elemanları yetiştirmeye yönelik bilgi ve beceri kazandırılacaktır.

2. Tüm dünyada olduğu gibi ülkemizde de haberleşme ağlarında yaygın olarak kullanılan Cisco ürünleri uygulamalarda kullanılacaktır. Kurs programı hem teorik hem de pratik çalışmalar içermektedir. Pratik çalışmalar teorik çalışmalarla bir bütün olarak uygulanacaktır. Uygulamalar toplam sürenin 1/3 ünden az olmayacaktır. Bu amaçla Cisco cihazlarıyla oluşturulmuş bir laboratuvar kullanılacaktır. Cihazların ayarlanması, yönetilmesi için kişisel bilgisayarlar kullanılacaktır. Öğrencilerin konuları anlama düzeyleri her hafta bitiminde yapılacak yoklama testleri ile değerlendirilecek ve eksiklikler hızla giderilecektir.

3. Kurs programı; bilgi birikimleri ve aldıkları eğitimin niteliği gereği elektronik, elektrik-elektronik, elektronik-haberleşme ve bilgisayar mühendisliği lisans diplomasına sahip veya elektronik ve bilgisayar öğretmenliği mezunlarınca "Uzman" vasfıyla doğrudan verilebilir. Bu, uzmanlık programının kalitesi için önemlidir. Alanında MEB onaylı "pekiyi" derece ile sertifika sahibi olmak kaydıyla, elektronik ve bilgisayar bölümü yüksekokul mezunları ve 4 senelik fakülte ya da eş değerinden mezun olanlar da eğitim verebilirler.

4. Programda, konuların son derece güncel ve teknik olması nedeniyle çok sayıda İngilizce terim kullanılmıştır. Bu nedenle kursiyer adaylarının okuduğunu anlayacak düzeyde İngilizce bilip bilmediği hususunda kendi beyanı esas alınacaktır. Ancak, kurs esnasında içerikteki hâlihazırda kabul görmüş ve ileride yerlerini alabilecek Türkçe terim karşılıklarının da kullanımına özel bir hassasiyet gösterilecektir.

5. Kurs sürecinde aktarılacak bilgilerin, çok kritik yerler de dahil olmak üzere çok geniş bir kullanım alanı bulunması nedeniyle ulusal çıkarlarımıza uygun şekilde kullanılmasına, kötü niyetli kullanımlar konusunda yasal dayanaklarıyla birlikte uyarıların yapılmasına özellikle dikkat edilmesi gerekmektedir. Benzer şekilde çevresel koşulların korunması ve mesleki etik konusunda bilinçlendirmeye özen gösterilmelidir.

6. Kurs programına katılacaklar için, eğitim kurumu "düzey belirleme" sınavı yapabilecek ve sınav sonucunda, katılımcılar programdaki ünitelerden yeterli olduğu konulardan başarılı sayılacak, başarısız olduğu ünitelerden eğitime devam edecektir. Ancak kursiyer bütün ünitelerden başarılı olsa bile, program süresinin en az ¼' ü kadar; genel tekrar ve bilgilerini yenileme kapsamında eğitim görecektir.

PROGRAMIN SÜRESİ

Hafta içi ve hafta sonu ders programı, toplam saat korunarak kurs müdürlüğünce düzenlenebilir.

1. **Hafta içi**
   Haftalık süre : Günde 6 saat X 5 gün = 30 saat
   Toplam süre : 3 hafta X 30 Saat = 90 saat
2. **Hafta sonu**
   Haftalık süre : Günde 5 saat X 2 gün = 10 saat
   Toplam süre : 9 hafta X 10 saat= 90 saat

PROGRAMIN İÇERİĞİNİN TOPLAM KURS SÜRESİNE GÖRE HAFTALIK DAĞILIMI
HAFTA İÇİ

1. HAFTA

A. YÖNLENDİRME PROTOKOLLERİ

1. EIGRP Ayarı
   a. EIGRP tanıtımı
   b. EIGRP kurulumu ve doğrulaması

c. İleri düzey EIGRP seçeneklerinin ayarı
ç. EIGRP kimlik doğrulama (Authentication) ayarı
d. Kurum ağında EIGRP kullanımı

2. OSPF Ayarı
   a. OSPF protokolünün tanıtımı
   b. OSPF paket tipleri
   c. OSPF yönlendirme ayarı
   ç. OSPF ağ tipleri
   d. Link State Advertisement (LSA) algoritması
   e. OSPF route summarization ayarı
   f. OSPF'te özel area tiplerinin ayarı
   g. OSPF kimlik doğrulama (authentication) ayarı
3. IS-IS Protokolü
   a. IS-IS ve Integrated IS-IS yönlendirme tanıtımı
   b. IS-IS yönlendirme operasyonu
   c. Temel Integrated IS-IS ayarı

B. ROUTING DUYURULARINA MÜDAHALE ETME

1. Çoklu IP Yönlendirme Protokolü Kullanan Ağları Yönetme
2. "Route Redistribution" Ayarı ve Doğrulaması
3. Yönlendirme Duyuruları Trafiğininin Ayarı
4. İleri Düzey IOS Özelliklerinin Gerçekleştirimi: DHCP Ayarı

C. TEMEL BGP AYARI

1. Genel BGP Kavramları ve Terminolojisi
2. EBGP ve IBGP Açıklamaları
3. Temel BGP Operasyonunun Ayarı
4. BGP Path Seçimi
5. Temel BGP Path Seçimine Müdahale Etmek İçin "Route Map" Kullanımı

2. HAFTA

A. IPv6 GERÇEKLEŞTİRİMİ

1. IPv6 Tanıtımı
2. IPv6 Adres Tanımı
3. Dinamik IPv6 Adreslerin Gerçekleştirilmesi
4. OSPF Ve Diğer Yönlendirme Protokolleriyle IPv6'nın Birlikte Kullanılması
5. IPv6 Ve IPv4'ün Birlikte Kullanımı

B. KAMPÜS AĞINA GİRİŞ

1. Kurulum Ağının Parçası Olarak Kampüs Ağı
2. Hiyerarşik Olamayan Ağda, Cihazlar
3. 2. Katman Ağ Sorunları
4. Çok Katmanlı Anahtarlama (Multilayer Switch)
5. Hiyerarşik Olmayan Ağda Çok Katmanlı Anahtarlama ve VLAN Sorunları

6. “Enterprise Composite Modeli”
    a. Erişim düzeyi (Building Access)
    b. Dağıtım düzeyi Building Distribution
    c. Sunucu kümesi (Server Farm)
    ç. Kampüs çekirdeği (Campus Core)
    d. Ağ yönetimi
7. “Enterprise Composite Model” in faydaları
8. “Campus Infrastructure” Modeli

C. SANAL AĞ TANIMLAMASI (VLAN)

1. VLAN Yapıları İçin Egzersizler
    a. Kötü tasarlanmış bir ağdaki sorunlar
    b. İşletme görevlerini VLAN’larla gruplama
2. VLAN Fonksiyonlarının İş Ortamında Kullanımı
    a. “Interconnection” teknolojileri
    b. Araç ve kablo gereksinimlerini belirleme
    c. Hiyerarşik ağlarda VLAN’lar
    ç. Kaynaktan hedefe trafik
    d. Anahtarlama ara birimlerinin gözden geçirilmesi
3. Bir Hierarchical Ağ İçinde “Mapping VLAN”
4. Kaynaktan Hedefe Giden Trafiğin İncelenmesi
5. Switch Ara Birim Ayarlarını Gözden Geçirme
6. VLAN Gerçekleştirimi
    a. Kurum ağında VLAN’ların faydaları
    b. Yerel (Local) VLAN’lar
    c. Uçtan uca (end–to–end) VLAN
    ç. VLAN ayar modları
    d. VLAN erişim portu
    e. VLAN gerçekleştirim komutları
    f. VLAN gerçekleştirimi
7. Trunk Gerçekleştirimi
    a. VLAN Trunk
    b. ISL Trunkları
    c. IEEE 802.1Q Trunkları
    ç. IEEE 802.1Q Native VLAN
    d. IEEE 802.1Q Native VLAN ile ilgili sorunlar
    e. VLAN aralıkları
8. VLAN Aralıkları Ayarları
    a. Trunk ayar komutları
    b. Trunk ayarı
    c. DTP (Dynamic Trunking Protocol) ayarları
9. VTP İle VLAN Bilgilerini Yayma
    a. “VTP Domain”
    b. VTP protokolü

c. VTP modları
ç. VTP pruning
d. VTP işleyişi
e. VTP ayar komutları
f. VTP yönetim domain ayarı
g. Mevcut VTP yapısına yeni anahtar ekleme

10. Genel Trunk Hat Problemlerinin Çözümü

Ç. SPANNING TREE PROTOKOLÜ GERÇEKLEŞTİRİMİ

1. Spanning Tree Protokolü (STP)
   a. Şeffaf köprüler (Transparent Bridges)
   b. Döngüleri (Loop) belirleme
   c. Döngülerin oluşmadığı ağlar
   ç. IEEE 802.1d Spanning Tree Protokolü (STP)
   d. Kök köprü (Root Bridge)
   e. Portların rolleri
   f. STP üzerine geliştirilmiş ilave fonksiyonlar
2. STP Yönlendirme Döngülerini Önleme
   a. Tek yönlü hat hatası
   b. Döngü koruyucu (Loop Guard)
   c. Tek yönlü hatlar yüzünden STP hatalarının oluşmasını engelleme
   ç. UDLD ve döngü koruyucu ayarı
3. Rapid Spanning Tree Protokolünün (RSTP) Gerçekleştirimi
   a. RSTP
   b. RSTP port durumları
   c. RSTP port rolleri
   ç. Kenar port (Edge Port)
   d. RSTP link tipleri
   e. RSTP BPDU paketleri
   f. RSTP "Proposal" ve "Agreement" işlemleri
   g. RSTP yapı değişikliği
   ğ. RSTP komutları
   h. RSTP komutlarının uygulanması
4. Multiple Spanning Tree Protokolün (MSTP) Gerçekleştirimi
   a. MSTP
   b. MSTP region
   c. Extended system ID
   ç. 802.1Q ve MSTP bölgeleri arasındaki etkileşim
   d. MSTP komutları
   e. MSTP ayarı ve doğrulaması
5. "Link Aggregation" ve "EtherChannel" Ayarı
   a. EtherChannel nedir?
   b. PAGP ve LACP protokolleri
   c. EtherChannel ayarı

ç. EtherChannel kullanarak "Port Channel" ayarı
d. EtherChannel üzerinde yük dağılımı ayarı

D. VLAN'LAR ARASI ROUTING GERÇEKLEŞTİRİMİ

1. VLAN'lar Arası Yönlendirme
   a. Çok katmanlı anahtar
   b. 2. katman anahtar yönlendirme işlemi
   c. Harici yönlendirici kullanarak VLAN'lar arası trafik taşıma (InterVLAN)
   ç. Harici yönlendirici kullanarak VLAN'lar arası trafik taşıma (InterVLAN) ayar komutları
2. CEF Tabanlı MLS
   a. 3. katman anahtarlama
   b. CEF tabanlı MLS
   c. MLS paket yönlendirme işlemi
   ç. CEF ayar komutları
   d. CEF tabanlı MLS çalıştırma
   e. Tipik CEF problemleri ve çözümleri
   f. CEF sorun giderme komutları
   g. CEF tabanlı MLS sorun giderme
3. VLAN'lar Arası Yönlendirmeyi Çalıştırma
   a. 3. katman anahtarda "Virtual Interface"
   b. 3. katman anahtarda "Routed Interface"
   c. 3. katman anahtarda VLAN'lar arası trafik taşıma (InterVLAN) ayar komutları

E. KAMPUS AĞININ ERİŞİLEBİLİRLİĞİNİ ARTIRMA

1. HSRP Kullanarak 3. Katman Yedeklilik Sağlama
   a. Yönlendirici yedekleme işlemi
   b. Yönlendirme sorunları
   c. HSRP nedir?
   ç. HSRP operasyonu
   d. HSRP durumları (States)
   e. HSRP ayar komutları
   f. HSRP'yi etkin kılma
2. VRRP ve GLBP Kullanarak 3. Katman Yedeklilik Sağlama
   a. VRRP operasyonu
   b. GLBP operasyonu
   c. VRRP ve GLBP'yi etkin kılma
   ç. VRRP ve GLBP ayarı
3. Modüler Switch'lerde Yedek Donanım ve Yazılım Gerçekleştirimi
   a. "Virtual Router Redundancy"
   b. "Supervisor Redundancy"
   c. Yedek "Supervisor Engine" ayar komutları

ç. Yedek “Supervisor Engine” gerçekleştirimi
d. Cisco Catalyst 6500 anahtarlar
e. “Single” ve “Dual” yönlendirici modları
f. SRM Ve SSM kullanarak hata dayanıklılığını artırma
g. Durmaksızın yönlendirme
ğ. NSF’le birlikte çalışan protokoller
h. NSF ve SSO kullanarak hata dayanıklılığını artırma
ı. NSF ayarı

4. Yedekli Güç Kaynağı Gerçekleştirimi
   a. Yedekli güç kaynağı ayarı
   b. Yüksek kullanılabilirlik ayarı doğrulaması
   c. Yük paylaşımı (Load Sharing)
   ç. HSRP verimliliği artırma seçenekleri
   d. HSRP ince ayarları
   e. HSRP “Debug” komutları
   f. HSRP ayarı hata düzeltmesi

F. KAMPÜS AĞINDA SERVİS KAYIPLARINI VE VERİ HIRSIZLIĞINI EN AZA İNDİRME

1. Anahtar Güvenliği
   a. Anahtar güvenlik konularının gözden geçirilmesi
   b. Anahtar atak kategorileri
   c. “MAC Flood” atak
   ç. “Port Security”
   d. “Port Security” ayarı
   e. “Sticky MAC” adreslerle port security
   f. İzinsiz erişim
   g. IEEE 802.1x port tabanlı kimlik doğrulama
2. VLAN ataklarına karşı koruma
   a. “VLAN hopping”
   b. “VLAN hopping” in üstesinden gelme
   c. VLAN erişim listeleri (VACL)
   ç. VACL ayarı
   d. Private VLAN (PVLAN)
   e. PVLAN ayarı
3. “Spoof” Ataklarına Karşı Korunma
   a. “DHCP Spoof” atağı
   b. “DHCP Snooping” kavramı
   c. “DHCP Snooping” ayar komutları
   ç. “MAC Spoof” atağı
   d. Address Resolution Protocol (ARP)
   e. Dinamik ARP denetleme ayar komutları
   f. “ARP Spoofing” ataklarına karşı korunma
4. Anahtarların Güvenliğini Artırma

a. Cisco Discovery Protokol'ündeki zaaflar (CDP)
b. "Secure Shell" zaafları
c. Telnet protokolünün zaafları
ç. VTY erişim listeleri
d. Erişim listelerini VTY'ye uygulamak için komutlar

5. STP Güvenlik Mekanizmaları
   a. STP operasyonunu koruma
   b. "BPDU Guard" ayarı
   c. "BPDU Filtering" ayarı
   ç. "Root Guard" kavramı
   d. "Root Guard" konfigürasyon komutları
   e. "Root Guard" ayarı

3. HAFTA

A. GÜVENLİK GÜÇLENDİRMESİ

1. Ağ Ataklarını Bertaraf Etme
   a. "Cisco self –defending" ağ stratejisi
   b. Kuruluşların savunma yapması gereken atak tipleri
   c. "Reconnaissance" ataklarının üstesinden gelme (packet sniffer, port scan, ping sweep, internet information query)
   ç. Access ataklarının üstesinden gelme (password attack, trust exploitation, buffer overflow, port redirection, man–in–the–middle)
   d. DoS ataklarının üstesinden gelme (IP spoofing ve DDoS)
   e. Worm, virus ve trojan horse ataklarının üstesinden gelme
   f. Uygulama (application) katmanı ataklarının üstesinden gelme
   g. Konfigürasyon yönetim protokollerinin zayıf noktaları ve bu zayıflıkların üstesinden gelme
   ğ. Ağ zayıflıklarını ve tehditlerini bulmak için kullanılabilecek açık kaynak araçlar
2. Kullanılmayan Cisco Yönlendirici Ağ Servislerini ve Ara Birimlerini Kapatma
   a. Ağ ataklarına karşı zayıf olan router servisleri ve ara birimleri
   b. "Auto secure" komutu kullanarak Cisco yönlendiriciye erişim güvenliğini arttırma
   c. Cisco yönlendirici üzerinde "auto secure" ayarı
   ç. Cisco yönlendirici komut satırındaki "auto secure" komutu ile "SDM security audit" sihirbazında bulunan "one-step lockdown" modu karşılaştırması
3. Cisco Yönlendirici Kurulumunu ve İdari Erişimi Daha Güvenli Hâle Getirme
   a. Şifre ayarları
   b. Başarısız login oranı belirleme ve gelişmiş "IOS login" özelliklerini kullanma
   c. Zaman aşımlarını (Timeout) belirleme

ç. Çoklu "privilege" seviyeleri belirleme
d. "Banner" mesajı ayarı
e. "Role – based CLI" ve temel "CLI view" ayarı için komutlar
f. "Cisco IOS boot image" ve ayar dosyalarını güvenceye alma

4. Tehdit ve Atakları ACL'lerle Bertaraf Etme
   a. Yönlendiriciler tarafından kullanılan IP ACL tipleri
   b. Router ara birimleride ACL uygulamaları
   c. Ağdaki tehditlerin üstesinden gelmek için ACL ile trafik filtreleme
   ç. Tehditlerin üstesinden gelmek için ACL gerçekleştirimi
   d. DDoS ataklarının etkisini azaltmak için router ACL ayarı
   e. Çoklu ACL işlevlerini iki veya üç ACL'de toplama
   f. ACL hazırlarken dikkat edilecek bazı hususlar
5. İdari ve Raporlama Özelliklerini Güvenceye Alma
   a. Ağ cihazlarında güvenli yönetim ve raporlama ayarı yaparken dikkat edilecek hususlar
   b. Güvenli yönetim ve raporlama mimarisini etkileyen faktörler
   c. Güvenli yönetim ve raporlama için "SSH server" kurulumu
   ç. Ağ güvenliğinde "syslog" özelliğinin ne kadar önemli olduğu
   d. Cisco router üzerinde "syslog" ayarı
   e. SNMPv3'te yer alan güvenlik özellikleri
   f. Kimlik doğrulama ile birlikte NTP client ayarı
   g. Cisco yönlendiricileri NTP server olarak ayarlama

B. KAMPÜS ANAHTARLARINDA SES (VOIP) AYARI

1. Kampüs Ağında Ses Gerçekleştirimi İçin Planlama
   a. Birleştirilmiş ağın faydaları
   b. VoIP ağ bileşenleri
   c. Ses ve veri trafik özellikleri
   ç. Voıp çağrı akışı
   d. "Auxiliary VLAN"
   e. "Quality of Service (QoS)"
   f. VoIP için yüksek kullanılabilirliğin önemi
   g. VoIP desteği için güç gereksinimleri
2. Ses Trafiğini Kampüs Ağına Yerleştirilmesi
   a. QoS güven sınırları
   b. "LAN-Based" sınıflandırma ve işaretleme
   c. Cisco IP telefon takacak şekilde anahtar ayarı yapma
   ç. "AutoQoS VoIP" nedir?
   d. Cisco anahtarları üzerinde "AutoQoS VoIP" ayarı yapma
3. Temel VoIP Konfigürasyonu
4. Temel IP Telefon Kavramları ve Uygulamaları

C. IP QoS'e GİRİŞ

1. QoS'e Giriş
   a. Ağlarda, anahtar kalite unsuru
   b. Düşük bant genişliğinin QoS üzerindeki negatif etkisi ve bant genişliğini etkili şekilde arttırmanın yolları
   c. End-to–end gecikmenin QoS üzerindeki negatif etkisi ve gecikmeyi etkili şekilde azaltmanın yolları
   ç. Ağdaki trafiğe göre QoS tanımlama
   d. QoS politikası gerçekleştiriminde kullanılan üç adım
   e. Ağda trafiğin, tipine göre nasıl ayırt edildiği ve bu tiplerin QoS trafik sınıflandırmasında nasıl kullanıldığı
   f. Trafik sınıflarının tanımlanmasından sonra QoS politikalarının tanımlanması
2. Qos Gerçekleştirimi İçin Modellerin Tanımlanması
   a. Ağda QoS sağlamak için kullanılan modeller
   b. "Best effort" modelinin başlıca özellikleri
   c. IntServ modelinin başlıca özellikleri
   ç. RSVP sayesinde IntServ nasıl sağlanır
   d. DiffServ modelinin başlıca özellikleri
3. Qos Gerçekleştirim Metotları
   a. QoS ayarı yapmak ve gözlemlemek için metotlar
   b. QoS ayarında CLI metodu
   c. QoS ayarında MQC metodu
   ç. QoS ayarında AutoQoS metodu
   d. Cisco SDM QoS sihirbazı

Ç. POWER on ETHERMET TEKNOLOJİLERİ

1. PoE nasıl çalışır
2. Güç (power) ihtiyacı olan cihazların tespiti
3. Cihazlara güç sağlama
4. PoE konfigürasyonu
5. PoE testi

D. WIRELESS KULLANICI ERİŞİMİ

1. Kablosuz Ağlara Giriş (WLAN)
   a. WLAN Nedir?
   b. LAN ve WLAN arasındaki benzerlikler
   c. LAN ve WLAN arasındaki farklar
   ç. WLAN bileşenleri
   d. WLAN teknolojileri gerçekleştirimi
   e. Access point blokları ile WLAN yapıları
   f. Köprü blokları ile WLAN yapıları
   g. Kablosuz ağ gerçekleştirimleri
2. Kablosuz Teorisi ve Standartları

a. RF temelleri
b. WLAN matematiği
c. Anten tipleri
ç. WLAN'ları düzenleyen merciler
d. IEEE 802.11 standartları
e. 2.4 Ghz bandında IEEE 802.11 standartları
f. IEEE 802.11a
g. IEEE 802.11 standartlarını karşılaştırma

3. WLAN Gerçekleştirimi
   a. 802.11b/g kanal yeniden kullanımı
   b. 802.11a kanal yeniden kullanımı
   c. WLAN egzersizleri
   ç. Güç gerçekleştirimi
4. Cisco WLAN
   a. Kuruluşlarda WLAN sorunları
   b. Cisco WLAN'a genel bakış
   c. "Autnomous" ve "lightweight" WLAN karşılaştırması
   ç. "Core" ve "advanced feature" roaming karşılaştırması
   d. "Split MAC" mimarisi
   e. "LWAPP access point" ilişkilendirmesi
   f. "WLAPP" ve "autonomous AP'leri birlikte kullanma
5. Cisco Kablosuz Kullanıcıları
   a. Wireless client ilişkilendirmesi
   b. "Open authentication"
   c. "Pre-shared key" kimlik denetimi (authentication WEP)
   ç. WLAN güvenlik tanıtımı
   d. "Cisco client" kartları
6. Temel WLAN Ayarı
   a. WLAN ayarı için ara birimler
   b. "Controller"a bağlanma
   c. "Controller" ayarı
   ç. "Controller" ayarı doğrulaması

E. WIRELESS ÖLÇEKLENEBİLİRLİK GERÇEKLEŞTİRİMİ

1. WLAN QoS Gerçekleştirimi
   a. WLAN QoS'e olan ihtiyaç
   b. WLAN QoS
   c. Bugünkü WLAN QoS gerçekleştirimleri
   ç. WLC kullanarak LightWeight AP üzerinde QoS ayarı
2. IEEE 802.1x Protokolü
   a. WLAN güvenlik standartlarına olan ihtiyaç ve WLAN güvenliğinin önemi
   b. "Encryption" ve "authentication" arasındaki fark
   c. Enhanced 802.11 güvenlik ve temel 802.11 güvenlik

ç. “802.1x authentication” temel kavramları
d. EAP Cisco wireless
e. EAP-fast
f. EAP-TLS
g. EAP-PEAP
ğ. WPA kimlik doğrulamasının işleyişi

3. LightWeight Access Point’ler Üzerinde “encryption” ve “authentication” Ayarı
   a. Controller üzerinde “open authentication” ayarı
   b. Controller üzerinde “pre-shared key authentication” ayarı
   c. Controller üzerinde “web authentication” ayarı
   ç. Controller üzerinde 802.1x ayarı
4. WLAN Yönetimi
   a. Wireless çözümlerin karşılaştırması
   b. Cisco’nun WLAN gerçekleştirimi
   c. WLAN kurulumu için gerekli bileşenler arasındaki hiyerarşi
   ç. WLSE temel özellikleri
   d. Cisco WCS temel özellikleri
   f. Cisco WCS tracking seçenekleri
   e. WLAN yönetimi için monitor tab kullanımı
   f. “2700 location appliance” işlevi
   g. Temel Cisco WCS ayarı
   ğ. WCS veritabanı üzerinde “map” ekleme, değiştirme ve kullanma
   h. “Cisco WCS rogue AP” metodu

HAFTA SONU

1. HAFTA

- **YÖNLENDİRME PROTOKOLLERİ**

1. EIGRP Ayarı
   a. EIGRP tanıtımı
   b. EIGRP kurulumu ve doğrulaması
   c. İleri düzey EIGRP seçeneklerinin ayarı
   ç. EIGRP kimlik doğrulama (Authentication) ayarı
   d. Kurum ağında EIGRP kullanımı

2. HAFTA

2. OSPF Ayarı
   a. OSPF protokolünün tanıtımı
   b. OSPF paket tipleri
   c. OSPF yönlendirme ayarı
   ç. OSPF ağ tipleri
   d. Link State Advertisement (LSA) algoritması
   e. OSPF route summarization ayarı
   f. OSPF’te özel area tiplerinin ayarı
   g. OSPF kimlik doğrulama (authentication) ayarı

3. IS-IS Protokolü
    a. IS-IS ve Integrated IS-IS yönlendirme tanıtımı
    b. IS-IS yönlendirme operasyonu
    c. Temel Integrated IS-IS ayarı

3. HAFTA

A. ROUTING DUYURULARINA MÜDAHALE ETME

1. Çoklu IP Yönlendirme Protokolü Kullanan Ağları Yönetme
2. "Route Redistribution" Ayarı ve Doğrulaması
3. Yönlendirme Duyuruları Trafiğininin Ayarı
4. İleri Düzey IOS Özelliklerinin Gerçekleştirimi: DHCP Ayarı

B. TEMEL BGP AYARI

1. Genel BGP Kavramları ve Terminolojisi
2. EBGP ve IBGP Açıklamaları
3. Temel BGP Operasyonunun Ayarı
4. BGP Path Seçimi
5. Temel BGP Path Seçimine Müdahale Etmek İçin "Route Map" Kullanımı

4. HAFTA

A. IPv6 GERÇEKLEŞTİRİMİ

1. IPv6 Tanıtımı
2. IPv6 Adres Tanımı
3. Dinamik IPv6 Adreslerin Gerçekleştirilmesi
4. OSPF Ve Diğer Yönlendirme Protokolleriyle IPv6'nın Birlikte Kullanılması
5. IPv6 Ve IPv4'ün Birlikte Kullanımı

B. KAMPÜS AĞINA GİRİŞ

1. Kurulum Ağının Parçası Olarak Kampüs Ağı
2. Hiyerarşik Olamayan Ağda Cihazlar
3. 2. Katman Ağ Sorunları
4. Çok Katmanlı Anahtarlama (Multilayer Switch)
5. Hiyerarşik Olmayan Ağda, Çok Katmanlı Anahtarlama ve VLAN Sorunları
6. "Enterprise Composite Modeli"
    a. Erişim düzeyi (Building Access)
    b. Dağıtım düzeyi Building Distribution
    c. Sunucu kümesi (Server Farm)
    ç. Kampüs çekirdeği (Campus Core)
    d. Ağ yönetimi
7. "Enterprise Composite Model" in Faydaları
8. "Campus Infrastructure" Modeli

5. HAFTA

A. SANAL AĞ TANIMLAMASI (VLAN)

1. VLAN Yapıları İçin Egzersizler

a. Kötü tasarlanmış bir ağdaki sorunlar
b. İşletme görevlerini VLAN larla gruplama

2. VLAN Fonksiyonlarının İş Ortamında Kullanımı
   a. "Interconnection" teknolojileri
   b. Araç ve kablo gereksinimlerini belirleme
   c. Hiyerarşik ağlarda VLAN lar
   ç. Kaynaktan hedefe trafik
   d. Anahtarlama ara birimlerinin gözden geçirilmesi
3. Bir Hierarchical Ağ İçinde "Mapping VLAN"
4. Kaynaktan Hedefe Giden Trafiğin İncelenmesi
5. Switch Ara Birim Ayarlarını Gözden Geçirme
6. VLAN Gerçekleştirimi
   a. Kurum ağında VLAN ların faydaları
   b. Yerel (Local) VLAN lar
   c. Uçtan uca (end–to–end) VLAN
   ç. VLAN ayar modları
   d. VLAN erişim portu
   e. VLAN gerçekleştirim komutları
   f. VLAN gerçekleştirimi
7. Trunk Gerçekleştirimi
   a. VLAN Trunk
   b. ISL Trunkları
   c. IEEE 802.1Q Trunkları
   ç. IEEE 802.1Q Native VLAN
   d. IEEE 802.1Q Native VLAN ile ilgili sorunlar
   e. VLAN aralıkları
8. VLAN Aralıkları Ayarları
   a. Trunk ayar komutları
   b. Trunk ayarı
   c. DTP (Dynamic Trunking Protocol) ayarları
9. VTP İle VLAN Bilgilerini Yayma
   a. "VTP Domain"
   b. VTP protokolü
   c. VTP modları
   ç. VTP pruning
   d. VTP işleyişi
   e. VTP ayar komutları
   f. VTP yönetim domain ayarı
   g. Mevcut VTP yapısına yeni anahtar ekleme
10. Genel Trunk Hat Problemlerinin Çözümü

B. SPANNING TREE PROTOKOLÜ GERÇEKLEŞTİRİMİ

1. Spanning Tree Protokolü (STP)
   a. Şeffaf köprüler (Transparent Bridges)

b. Döngüleri (Loop) belirleme
c. Döngülerin oluşmadığı ağlar
ç. IEEE 802.1d Spanning Tree Protokolü (STP)
d. Kök köprü (Root Bridge)
e. Portların rolleri
f. STP üzerine geliştirilmiş ilave fonksiyonlar

2. STP Yönlendirme Döngülerini Önleme
   a. Tek yönlü hat hatası
   b. Döngü koruyucu (Loop Guard)
   c. Tek yönlü hatlar yüzünden STP hatalarının oluşmasını engelleme
   ç. UDLD ve döngü koruyucu ayarı
3. Rapid Spanning Tree Protokolünün (RSTP) Gerçekleştirimi
   a. RSTP
   b. RSTP port durumları
   c. RSTP port rolleri
   ç. Kenar port (Edge Port)
   d. RSTP link tipleri
   e. RSTP BPDU paketleri
   f. RSTP "Proposal" ve "Agreement" işlemleri
   g. RSTP yapı değişikliği
   ğ. RSTP komutları
   h. RSTP komutlarının uygulanması
4. Multiple Spanning Tree Protokolün (MSTP) Gerçekleştirimi
   a. MSTP
   b. MSTP region
   c. Extended system ID
   ç. 802.1Q ve MSTP bölgeleri arasındaki etkileşim
   d. MSTP komutları
   e MSTP ayarı ve doğrulaması
5. "Link Aggregation" ve "EtherChannel" Ayarı
   a. EtherChannel nedir?
   b. PAGP ve LACP protokolleri
   c. EtherChannel ayarı
   ç. EtherChannel kullanarak "Port Channel" ayarı
   d. EtherChannel üzerinde yük dağılımı ayarı

6. HAFTA

A. VLANLAR ARASI ROUTING GERÇEKLEŞTİRİMİ

1. VLAN lar Arası Yönlendirme
   a. Çok katmanlı anahtar
   b. 2. katman anahtar yönlendirme işlemi
   c. Harici yönlendirici kullanarak VLAN lar arası trafik taşıma (InterVLAN)
   ç. Harici yönlendirici kullanarak VLAN lar arası trafik taşıma (InterVLAN) ayar komutları

2. CEF Tabanlı MLS
    a. 3. katman anahtarlama
    b. CEF tabanlı MLS
    c. MLS paket yönlendirme işlemi
    ç. CEF ayar komutları
    d. CEF tabanlı MLS çalıştırma
    e. Tipik CEF problemleri ve çözümleri
    f. CEF sorun giderme komutları
    g. CEF tabanlı MLS sorun giderme
3. VLAN lar Arası Yönlendirmeyi Çalıştırma
    a. 3. katman anahtarda "Virtual Interface"
    b. 3. katman anahtarda "Routed Interface"
    c. 3. katman anahtarda VLAN lar arası trafik taşıma (InterVLAN) ayar komutları

B. KAMPUS AĞININ ERİŞİLEBİLİRLİĞİNİ ARTIRMA

1. HSRP Kullanarak 3. Katman Yedeklilik Sağlama
    a. Yönlendirici yedekleme işlemi
    b. Yönlendirme sorunları
    c. HSRP nedir?
    ç. HSRP operasyonu
    d. HSRP durumları (States)
    e. HSRP ayar komutları
    f. HSRP'yi etkin kılma
2. VRRP ve GLBP Kullanarak 3. Katman Yedeklilik Sağlama
    a. VRRP operasyonu
    b. GLBP operasyonu
    c. VRRP ve GLBP'yi etkin kılma
    ç. VRRP ve GLBP ayarı
3. Modüler Switch'lerde Yedek Donanım ve Yazılım Gerçekleştirimi
    a. "Virtual Router Redundancy"
    b. "Supervisor Redundancy"
    c. Yedek "Supervisor Engine" ayar komutları
    ç. Yedek "Supervisor Engine" gerçekleştirimi
    d. Cisco Catalyst 6500 anahtarlar
    e. "Single" ve "Dual" yönlendirici modları
    f. SRM Ve SSM kullanarak hata dayanıklılığını artırma
    g. Durmaksızın yönlendirme
    ğ. NSF le birlikte çalışan protokoller
    h. NSF ve SSO kullanarak hata dayanıklılığını artırma
    ı. NSF ayarı
4. Yedekli Güç Kaynağı Gerçekleştirimi
    a. Yedekli güç kaynağı ayarı
    b. Yüksek kullanılabilirlik ayarı doğrulaması

c. Yük paylaşımı (Load Sharing)
ç. HSRP verimliliği artırma seçenekleri
d. HSRP ince ayarları
e. HSRP "Debug" komutları
f. HSRP ayarı hata düzeltmesi

7. HAFTA

A. KAMPÜS AĞINDA SERVİS KAYIPLARINI VE VERİ HIRSIZLIĞINI EN AZA İNDİRME

1. Anahtar Güvenliği
   a. Anahtar güvenlik konularının gözden geçirilmesi
   b. Anahtar atak kategorileri
   c. "MAC Flood" atak
   ç. "Port Security"
   d. "Port Security" ayarı
   e. "Sticky MAC" adreslerle port security
   f. İzinsiz erişim
   g. IEEE 802.1x port tabanlı kimlik doğrulama
2. VLAN ataklarına karşı koruma
   a. "VLAN hopping"
   b. "VLAN hopping" in üstesinden gelme
   c. VLAN erişim listeleri (VACL)
   ç. VACL ayarı
   d. Private VLAN (PVLAN)
   e. PVLAN ayarı
3. "Spoof" Ataklarına Karşı Korunma
   a. "DHCP Spoof" atağı
   b. "DHCP Snooping" kavramı
   c. "DHCP Snooping" ayar komutları
   ç. "MAC Spoof" atağı
   d. Address Resolution Protocol (ARP)
   e. Dinamik ARP denetleme ayar komutları
   f. "ARP Spoofing" ataklarına karşı korunma
4. Anahtarların Güvenliğini Artırma
   a. Cisco Discovery Protokol'ündeki zaaflar (CDP)
   b. "Secure Shell" zaafları
   c. Telnet protokolünün zaafları
   ç. VTY erişim listeleri
   d. Erişim listelerini VTY'ye uygulamak için komutlar
5. STP Güvenlik Mekanizmaları
   a. STP operasyonunu koruma
   b. "BPDU Guard" ayarı
   c. "BPDU Filtering" ayarı
   ç. "Root Guard" kavramı

d. “Root Guard” konfigürasyon komutları
e. “Root Guard” ayarı

B. GÜVENLİK GÜÇLENDİRMESİ

1. Ağ Ataklarını Bertaraf Etme
   a. “Cisco self –defending” ağ stratejisi
   b. Kuruluşların savunma yapması gereken atak tipleri
   c. “Reconnaissance” ataklarının üstesinden gelme (packet sniffer, port scan, ping sweep, internet information query)
   ç. Access ataklarının üstesinden gelme (password attack, trust exploitation, buffer overflow, port redirection, man–in–the–middle)
   d. DoS ataklarının üstesinden gelme (IP spoofing ve DDoS)
   e. Worm, virus ve trojan horse ataklarının üstesinden gelme
   f. Uygulama (application) katmanı ataklarının üstesinden gelme
   g. Konfigürasyon yönetim protokollerinin zayıf noktaları ve bu zayıflıkların üstesinden gelme
   ğ. Ağ zayıflıklarını ve tehditlerini bulmak için kullanılabilecek açık kaynak araçlar
2. Kullanılmayan Cisco Yönlendirici Ağ Servislerini ve Ara Birimlerini Kapatma
   a. Ağ ataklarına karşı zayıf olan router servisleri ve ara birimleri
   b. “Auto secure” komutu kullanarak Cisco yönlendiriciye erişim güvenliğini arttırma
   c. Cisco yönlendirici üzerinde “auto secure” ayarı
   ç. Cisco yönlendirici komut satırındaki “auto secure” komutu ile “SDM security audit” sihirbazında bulunan “one-step lockdown” modu karşılaştırması
3. Cisco Yönlendirici Kurulumunu ve İdari Erişimi Daha Güvenli Hâle Getirme
   a. Şifre ayarları
   b. Başarısız login oranı belirleme ve gelişmiş “IOS login” özelliklerini kullanma
   c. Zaman aşımlarını (Timeout) belirleme
   ç. Çoklu “privilege” seviyeleri belirleme
   d. “Banner” mesajı ayarı
   e. “Role – based CLI” ve temel “CLI view” ayarı için komutlar
   f. “Cisco IOS boot image” ve ayar dosyalarını güvenceye alma
4. Tehdit ve Atakları ACL lerle Bertaraf Etme
   a. Yönlendiriciler tarafından kullanılan IP ACL tipleri
   b. Router ara birimleride ACL uygulamaları
   c. Ağdaki tehditlerin üstesinden gelmek için ACL ile trafik filtreleme
   ç. Tehditlerin üstesinden gelmek için ACL gerçekleştirimi
   d. DDoS ataklarının etkisini azaltmak için router ACL ayarı
   e. Çoklu ACL işlevlerini iki veya üç ACL’de toplama
   f. ACL hazırlarken dikkat edilecek bazı hususlar
5. İdari ve Raporlama Özelliklerini Güvenceye Alma

a. Ağ cihazlarında güvenli yönetim ve raporlama ayarı yaparken dikkat edilecek hususlar
b. Güvenli yönetim ve raporlama mimarisini etkileyen faktörler
c. Güvenli yönetim ve raporlama için "SSH server" kurulumu
ç. Ağ güvenliğinde "syslog" özelliğinin ne kadar önemli olduğu
d. Cisco router üzerinde "syslog" ayarı
e. SNMPv3'te yer alan güvenlik özellikleri
f. Kimlik doğrulama ile birlikte NTP client ayarı
g. Cisco yönlendiricileri NTP server olarak ayarlama

8. HAFTA

A. KAMPÜS ANAHTARLARINDA SES (VOIP) AYARI

1. Kampüs Ağında Ses Gerçekleştirimi İçin Planlama
   a. Birleştirilmiş ağın faydaları
   b. VoIP ağ bileşenleri
   c. Ses ve veri trafik özellikleri
   ç. Voıp çağrı akışı
   d. "Auxiliary VLAN"
   e. "Quality of Service (QoS)"
   f. VoIP için yüksek kullanılabilirliğin önemi
   g. VoIP desteği için güç gereksinimleri
2. Ses Trafiğini Kampüs Ağına Yerleştirilmesi
   a. QoS güven sınırları
   b. "LAN-Based" sınıflandırma ve işaretleme
   c. Cisco IP telefon takacak şekilde anahtar ayarı yapma
   ç. "AutoQoS VoIP" nedir?
   d. Cisco anahtarları üzerinde "AutoQoS VoIP" ayarı yapma
3. Temel VoIP Konfigürasyonu
4. Temel IP Telefon Kavramları ve Uygulamaları

B. IP QoS'e GİRİŞ

1. QoS'e Giriş
   a. Ağlarda, anahtar kalite unsuru
   b. Düşük bant genişliğinin QoS üzerindeki negatif etkisi ve bant genişliğini etkili şekilde arttırmanın yolları
   c. End-to–end gecikmenin QoS üzerindeki negatif etkisi ve gecikmeyi etkili şekilde azaltmanın yolları
   ç. Ağdaki trafiğe göre QoS tanımlama
   d. QoS politikası gerçekleştiriminde kullanılan üç adım
   e. Ağda trafiğin, tipine göre nasıl ayırt edildiği ve bu tiplerin QoS trafik sınıflandırmasında nasıl kullanıldığı
   f. Trafik sınıflarının tanımlanmasından sonra QoS politikalarının tanımlanması
2. Qos Gerçekleştirimi İçin Modellerin Tanımlanması
   a. Ağda QoS sağlamak için kullanılan modeller

b. “Best effort” modelinin başlıca özellikleri
c. IntServ modelinin başlıca özellikleri
ç. RSVP sayesinde IntServ nasıl sağlanır?
d. DiffServ modelinin başlıca özellikleri

3. Qos Gerçekleştirim Metotları
   a. QoS ayarı yapmak ve gözlemlemek için metotlar
   b. QoS ayarında CLI metodu
   c. QoS ayarında MQC metodu
   ç. QoS ayarında AutoQoS metodu
   d. Cisco SDM QoS sihirbazı

C. POWER on ETHERMET TEKNOLOJİLERİ

1. PoE nasıl çalışır?
2. Güç (power) ihtiyacı olan cihazların tespiti
3. Cihazlara güç sağlamak
4. PoE konfigürasyonu
5. PoE testi

9. HAFTA

A. WIRELESS KULLANICI ERİŞİMİ

1. Kablosuz Ağlara Giriş (WLAN)
   a. WLAN nedir?
   b. LAN ve WLAN arasındaki benzerlikler
   c. LAN ve WLAN arasındaki farklar
   ç. WLAN bileşenleri
   d. WLAN teknolojilerinin gerçekleştirimi
   e. Access point blokları ile WLAN yapıları
   f. Köprü blokları ile WLAN yapıları
   g. Kablosuz ağ gerçekleştirimleri
2. Kablosuz Teorisi ve Standartları
   a. RF temelleri
   b. WLAN matematiği
   c. Anten tipleri
   ç. WLAN ları düzenleyen merciler
   d. IEEE 802.11 standartları
   e. 2.4 Ghz bandında IEEE 802.11 standartları
   f. IEEE 802.11a
   g. IEEE 802.11 standartlarını karşılaştırma
3. WLAN Gerçekleştirimi
   a. 802.11b/g kanal yeniden kullanımı
   b. 802.11a kanal yeniden kullanımı
   c. WLAN egzersizleri
   ç. Güç gerçekleştirimi
4. Cisco WLAN

a. Kuruluşlarda WLAN sorunları
b. Cisco WLAN'a genel bakış
c. "Autnomous" ve "lightweight" WLAN karşılaştırması
ç. "Core" ve "advanced feature" roaming karşılaştırması
d. "Split MAC" mimarisi
e. "LWAPP access point" ilişkilendirmesi
f. "LWAPP" ve "autonomous AP'leri birlikte kullanma

5. Cisco Kablosuz Kullanıcıları
   a. Wireless client ilişkilendirmesi
   b. "Open authentication"
   c. "Pre-shared key" kimlik denetimi (authentication WEP)
   ç. WLAN güvenlik tanıtımı
   d. "Cisco client" kartları
6. Temel WLAN Ayarı
   a. WLAN ayarı için ara birimler
   b. "Controller"a bağlanma
   c. "Controller" ayarı
   ç. "Controller" ayarı doğrulaması

B. WIRELESS ÖLÇEKLENEBİLİRLİK GERÇEKLEŞTİRİMİ

1. WLAN QoS Gerçekleştirimi
   a. WLAN QoS'e olan ihtiyaç
   b. WLAN QoS
   c. Bugünkü WLAN QoS gerçekleştirimleri
   ç. WLC kullanarak LightWeight AP üzerinde QoS ayarı
2. IEEE 802.1x Protokolü
   a. WLAN güvenlik standartlarına olan ihtiyaç ve WLAN güvenliğinin önemi
   b. "Encryption" ve "authentication" arasındaki fark
   c. Enhanced 802.11 güvenlik ve temel 802.11 güvenlik
   ç. "802.1x authentication" temel kavramları
   d. EAP Cisco wireless
   e. EAP-fast
   f. EAP-TLS
   g. EAP-PEAP
   ğ. WPA kimlik doğrulamasının işleyişi
3. LightWeight Access Pointler Üzerinde "Encryption" ve "Authentication" Ayarı
   a. Controller üzerinde "open authentication" ayarı
   b. Controller üzerinde "pre-shared key authentication" ayarı
   c. Controller üzerinde "web authentication" ayarı
   ç. Controller üzerinde 802.1x ayarı
4. WLAN Yönetimi
   a. Wireless çözümlerin karşılaştırması
   b. Cisco'nun WLAN gerçekleştirimi
   c. WLAN kurulumu için gerekli bileşenler arasındaki hiyerarşi

ç. WLSE temel özellikleri
d. Cisco WCS temel özellikleri
f. Cisco WCS tracking seçenekleri
e. WLAN yönetimi için monitor tab kullanımı
f. "2700 location appliance" işlevi
g. Temel Cisco WCS ayarı
ğ. WCS veritabanı üzerinde "map" ekleme, değiştirme ve kullanma
h. "Cisco WCS rogue AP" metodu

ÖLÇME VE DEĞERLENDİRMEYLE İLGİLİ ESASLAR

Kurs bitiminde MEB Özel Öğretim Kurumları Genel Müdürlüğünün Özel Yabancı Dil, Meslek ve Teknik Kursları Bitirme Sınavları ve Kurslarda Uygulanacak Esaslar dikkate alınarak teorik (yazılı) ve uygulamalı sınav yapılır. Sınavların her birinin değerlendirmesi, aşağıda belirtilen puanlama esaslarına göre gerçekleştirilir. Sınav sonucunda başarılı olanlara Millî Eğitim Bakanlığı onaylı "Kurs Bitirme Belgesi" verilir.

PUAN	NOT	DERECE
0-44	D	Başarısız
45-69	C	Orta
70-84	B	İyi
85-100	A	Pekiyi

PROGRAMIN UYGULANMASINDA KULLANILACAK ÖĞRETİM ARAÇ-GEREÇLERİ

Yardımcı Kaynaklar
Ders öğretmenince hazırlanacak ders notları (baskı yoluyla veya CD ile) dağıtılacaktır.
Kullanılacak Araç ve Gereçler
Simülatör/Emülatör ya da uzaktan laboratuvar kullanımı sadece yardımcı araç olarak kullanılabilir.

1. Öğretmen bilgisayarı
2. Öğrenci sayısı kadar öğrenci bilgisayarı
3. 1 adet server
4. Projeksiyon cihazı
5. Bir adet yazıcı
6. 1 adet Cisco CallManager
7. 1 Adet ACS Server
9. 1 Adet Cisco Wireless Controller
10. 3 adet Cisco LWAPP
11. Öğrenci sayısının yarısı kadar Cisco Autonomous AP
12. Öğrenci sayısı kadar "Cisco IP Phone" ve adaptörü
13. Öğrenci sayısı kadar Analog telefon ve kabloları

14. Öğrenci başına 3 adet Cisco Yönlendirici (Router) cihazı (En az bir tanesinde 1 FXS kartı)
15. Öğrenci başına 3 adet DTE ve 3 adet DCE kablosu
16. Öğrenci başına 3 adet çapraz ve 1 adet düz bağlı enaz CAT 5 standardında kablo
17. Öğrenci başına en az 2 adet Cisco L2 Anahtar (Switch) ve 1 adet Cisco L3 Anahtar (Switch) cihazı
18. Tüm cihazları besleyen kesintisiz güç kaynağı
19. 1 Adet öğrenci sayısı kadar portu olan Cisco DSLAM cihazı
20. Öğrenci sayısı kadar Cisco ADSL Router
21. Jeneratör
22. 2 Mbps ADSL internet bağlantısı

Kısaltmalar

802.1q	: VLAN tagging
AAA	: Authentication, Authorization and Accounting
AAR	: Automated alternate routing
ACE	: Access Control Entry
ACL	: Access Control List
ACL	: Access Control List
AFI	: Authority and Format Identifier
ARP	: Address Resolution Protocol
AVVID	: Architecture for Voice, Video and Integrated Data
BECN	: Backward Explicit Congestion Notification
BGP	: Border Gateway Protocol
BPDU	: Bridge Protocol Data Unit
bps	: Bit per second
BRI	: Basic Rate Interface - Basit Oran Arayüzü
BUS	: Broadcast and Unknown Server
BVI	: Bridge-group Virtual Interface
CAC	: Call Admission Control
CAM	: Content Addressable Memory
CAR	: Committed Access Rate
CBWFQ	: Class Based Waited Fair Queue
CCNA	: Cisco Certificated Network Associate
CCNP	: Cisco Certificated Network Professional
CDP	: Cisco Discovery Protocol
CE	: Customer Equipment
CEF	: Cisco Express Forwarding
CGMP	: Cisco Group Management Protocol
CHAP	: Challenge-Handshake Authentication Protocol
CHAP	: Challenge Handshake Authentication Protocol
CIR	: Committed Information Rate
CLI	: Command Line Interface

CoS : Class of Service
CRC : Cyclic Redundancy Check
cRTP : Compressed Real Time Protocol
CST : Common Spanning Tree
DCE : Data Communications Equipment
dCEF : distributed Cisco Express Forwarding
DDoS : Distributed Denial of Service
DDR : Dial-on-Demand Routing
DE : Discard Eligibility
DMZ : DeMilitarized Zone
DNS : Domain Name System
DoD : Department of Defense
DoD : Department of Defense
DOS : Denial of Service
DRAM : Dynamic RAM
DSCP : Differentiated Services Code Point
DSP : Digital Signal Processor
DTE : Data Terminal Equipment
DTP : Dynamic Trunking Protocol
DTR : Data Terminal Ready
EAP : Extensible Authentication Protocol
EAP-fast : Extensible Authentication Protocol-fast
EAP-PEAP : Extensible Authentication Protocol -Protected Extensible Authentication Protocol
EAP-TLS : Extensible Authentication Protocol-Transport Lecel Security
EEPROM : Electrically Erasable Programmable Read Only Memory
EIA : Electronic Industries Association
EIGRP : Enhanced Interior Gateway Routing Protocol
FECN : Forward Explicit Congestion Notification
FIFO : First In First Out
FR : Frame Relay
FSM : Feasible Successor Metrics
GLBP : Gateway Load Balancing Protocol
GRE : Generic Route Encapsulation
HDLC : High Level Data Link Protocol
HSRP : Hot Standby Routing Protocol
HTTP : Hypertext Terminal Protocol
ICC : Inter Card Communication
ICMP : Internet Control Message Protocol
IDS : Intruder Dedection System
IEEE : The Institute of Electrical and Electronics Engineers
IFS : IOS File System
IGMP : Internet Group Management Protocol
IGRP : Interior Gateway Routing Protocol

IKE : Internet Key Exchange
ILMI : Integrated Local Management Interface
IOS : Internetworking Operating System
IP : Internet Protocol
IPS : Intruder Preventing System
IPSec : IP Security
ISDN : Integrated Services Digital Network
IS-IS : Intermediate System-to-Intermediate System Intradomain Routing Protocol
IS-IS : Internediate System-to-Intemediate System
ISL : Inter-Switch Link
ISO : International Organization of Standardization
L2TP : Layer 2 Tunnel Protocol
LACP : Link Aggregration Protocol
LAN : Local Area Network
LAPB : Link Access Procedure Balanced
LCP : Link Control Protocol
LCP : Link Control Protocol
LDA : Local Director Acceleration
LES : LAN Emulation Server
LFIB : Label Forwarding Information Base
LLC : Logical Link Control
LLQ : Low Latency Queue
LMI : Link Management Interface
LSA : Link State Advertisement
LWAPP : LightWeight Access Point Protocol
MAC : Media Access Control
MAN : Metropolitan Area Network
MD5 : Message Digest 5
MIB : Management Information Base
MII : Media-Independent Interface
MLS : Multilayer Switching
MLSE : Maintenance Loop Signaling Entity
MOP : Maintenance Operation Protocol
MOTD : Message-Of-The-Day
MQC : Modular QoS
MSDP : Multicast Source Discovery Protocol
MST : Multiple Spanning Tree
MSTI : MST Instance
MSTP : Multiple Spanning Tree
MTU : Maximum Transmission Unit
NAT : Network Address Translation
NBAR : Network Based Application Recognition
NDE : NetFlow Data Export

NET : Network Entity Title
NetBIOS : Network Basic Input/Output System
NFFC : NetFlow Feature Card
NMP : Network Management Processor
NSAP : Network Service Access Point
NSF : Non-Stop Forwarding
NSF : Nonstop Forwarding
NTP : Network Time Protocol
NVRAM : Nonvolatile RAM
OSI : Open System Interconnection
OSPF : Open Shortest Path First Protocol
OSPF : Open shortest path first
PACL : Port Access Control List
PAE : Port access entity
PAgP : Port Aggregation Protocol
PAP : Password authentication protocol
PAT : Port Address Translation
PBD : Packet buffer daughterboard
PBR : Policy Based Routing
PBX : Private Branch Exchange
PC : Personal Computer
PCM : Pulse code modulation
PDP : Policy decision point
PDU : Protocol data unit
PE : Provider Equipment
PEP : Policy enforcement point
PGM : Pragmatic General Multicast
PHY : Physical sublayer
PIB : Policy information base
PIM : Protocol Independent Multicast
PKI : Public Key Infrastructure
PoE : Power over Internet
PPP : Point-to-Point Protocol
PQ : Priority Queue
PRI : Primary Rate Interface
PSTN : Public Switching Telephone Network
PVC : Permenant Virtual Circuit
PVST : Per-VLAN Spanning Tree Protocol
PVST+ : Per VLAN Spanning Tree+
QM : QoS manager
QoS : Quality of Service
RADIUS : Remote Access Dial-In User Service
RAM : Random Access Memory
RCP : Remote Copy Protocol

RED : Random Early Detection
RF : Radio Frequency
RGMP : Router-ports Group Management Protocol
RIB : Routing Information Base
RIF : Routing Information Field
RIP : Router Information Protocol
RMON : Remote Network MONitor
ROM : Read-Only Memory
ROMMON : ROM Monitor
RP : Route Processor yada Rendezvous Point
RPC : Remote Procedure Call
RPF : Reverse Path Forwarding
RPR : Route Processor Redundancy
RR : Round robin
RSPAN : Remote SPAN
RST : Reset
RSTP : Rapid Spanning Tree, Real Time Streaming Protocol
RSVP : Resource Reservation Protocol
RTP : Realtime Transfer Protocol
SAID : Security Association Identifier
SAP : Service Access Point
SCM : Service Connection Manager
SCP : Switch-Module Configuration Protocol
SDEE : Security Device Event Exchange
SDLC : Synchronous Data Link Control
SDM : Security Device Manager
SFP : Small Form-factor Pluggable transceiver
SIMM : Single In-line Memory Module
SLB : Server Load Balancing
SLCP : Supervisor Line-Card Processor
SLIP : Serial Line Internet Protocol
SMDS : Software Management and Delivery Systems
SMTP : Simple Mail Transfer Protocol
SNMP : Simple Network Management Protocol
SPAN : Switched Port Analyzer
SRM : Service Resource Module
SSM : Security Service Module
SSO : Stateful Switchover
STP : Spanning Tree Protocol
SVC : Switched Virtual Circuit
SVI : Switched Virtual Interface
TACACS+ : Terminal Access Controller Access Control System Plus
TCAM : Ternary Content Addressable Memory
TCP : Transmission Control Protocol

TCP/IP : Transmission Control Protocol/Internet Protocol
TFTP : Trivial File Transfer Protocol
TLV : Type-Length-Value
TOS : Type of Service
TTL : Time To Live
UDLD : UniDirectional Link Detection
UDP : User Datagram Protocol
VACL : VLAN access control list
VAD : Voice Activity Detection
VCC : Virtual Channel Circuit
VCI : Virtual Circuit Identifier
VLAN : Virtual LAN
VLSM : Variable Lenght Subnet Mask
VMPS : VLAN Membership Policy Server
VoIP : Voice over IP
VPN : Virtual Private Network
VRF : VPN Routing and Forwarding
VRRP : Virtual Router Redundancy Protocol
VTP : VLAN Trunking Protocol
VTY : Virtual TeleType
VVID : Voice VLAN ID
WAN : Wide Area Network
WCS : Wireless Control System
WEP : Wired Equivalent Privacy
WFQ : Weighted FairQueueing
WLAN : Wireless LAN
WLC : Wireless LAN Controller
WLSE : Wireless LAN Solution Engine
WPA : Wi-Fi Protected Access
WRED : Weighted Random Early Detection
WRR : Weighted Round-Robin

Kavramlar Sözlüğü

802.1q : VLAN tagging protokol.
Accounting : Raporlama.
Advanced feature : İleri düzey özellikler.
Agreement : Anlaşma.
Appliance : Özel bir teknolojiyi donanımsal olarak gerçekleştiren cihaz.
Authentication : Kimlik doğrulama.
Authorization : Yetkilendirme.
Autnomous : Cisco AP lerde bir IOS türü (Bağımsız yönetilen).
Auxiliary VLAN : Yardımcı VLAN.
Banner : Bilgilendirme metni.
Best effort : Sıradan hizmet (QoS).
Bridge : Köprü.

Bridging : Köprüleme.
Buffer overflow : Tampon hafıza kapasitesinin aşımı.
Building access : Switchlerde bir erişim düzeyi.
Call agent : Telefon sisteminde çağrı yöneticisi.
Campus core : Kampüs çekirdeği.
Circuit-switched : Devre anahtarlama.
Cisco : Amerika kökenli, bir network firması.
Classfull : IP adreslemede sınıf gözeten.
Classification : Sınıflandırma.
Classless : IP adreslemede sınıf gözetmeyen (sınıfsız).
Composite metric : IGRP Protokolünde en iyi yol seçimi yapılması.
Congestion management : Sıkışma kontrolü (QoS).
Convergence : Routing protokllerinde netleşme.
Cost : Maliyet, bedel.
Count to infinity : Sonsuza dek sayma.
Defending : Savunma, Korunma.
Delay : Geçikme (QoS).
Dial-on-demand : İsteğe bağlı arama.
DiffServ : Differentiated Services (QoS).
Discontinuous : Süreksizlik.
Discovery : Keşif.
Distance vector : Bir yönlendirme protokolü (RIP ve IGRP tarafından kullanılır).
Edge port : Kenar port.
Encapsulation : Zarflama, Sarmalama, kapsülleme.
Encryption : Kripto.
End–to–end : Uçtan uca.
Enterprise : Kurumsal.
Ethernet : OSI L2 LAN protokolü.
Extended : Genişletilmiş
Filtering : Filitreleme, süzme.
Firewall : Güvenlik duvarı.
Frame-Relay : Bir OSI 2nci katman WAN protokolü.
IEEE 802.11a : Bir kablosuz ağ standartı (54 Mbps - 5 Ghz).
IEEE 802.11b : Bir kablosuz ağ standartı (11 Mbps - 2.4 Ghz).
IEEE 802.11g : Bir kablosuz ağ standartı (54 Mbps - 2.4 Ghz).
IEEE 802.11n : Bir kablosuz ağ standartı (54 Mbit/s to 600 Mbit/s - 2.4/5 Ghz).
Infrastructure : Alt yapı
Integrity : Bütünlük.
Interconnection : Ara bağlantı.
InterVLAN : VLAN lar arası
Jitter : Paket geçikme(delay) düzensizliği (QoS).
LightWeight : Cisco AP lerde bir IOS türü (Merkezi yönetilen).
Link efficiency : İletişim hattının daha verimli kullanılması (QoS).
Link state : Bir yönlendirme protokolü (OSPF ve IS-IS tarafından kullanılır).
Link state : Bir yönlendirme protokolü.

Load sharing : Yük paylaşımı.
Location : Yer.
Loop : Döngü.
Loop guard : Döngü koruyucu.
MAC : Medya erişim kontrolü.
MAC address : Medya erişim kontrolü adresi.
MAC flooding : Bir saldırı türü.
Man–in–the–middle : Ortadaki adam saldırısı.
Map : İlişkilendirme.
Marking : İşaretleme.
Multilayer Switch : Çok katmanlı anahtarlama.
Multipoint : Çoklu bağlantı noktası.
Multipoint : Ortadaki adam saldırısı.
Native VLAN : IEEE 802.1q'da tanımlı bir fonksiyon.
Network : Ağ.
One-step lockdown : Bir cihazı tek adımda güvenli hale getirmek.
Overhead : Yük.
Overload : Aşırı yüklenme.
Packet inspection : Paket kontrolü.
Password attack : Şifre çözme(kırma) girişimi.
Point-to-point : Uçtan-uca.
Poison reverse : Yönlendirme döngülerini önlemeye yarayan bir mekanizma.
Policy : Politika.
Port : Servis adresi.
Port (Interface) : Bağlantı noktası.
Port redirection : Port yönlendirme.
Pre-classify : Ön sınıflandırma.
Pre-shared key : Ön tanımlı anahtar.
Proposal : Öneri, teklif.
Proxy : Temsilci.
Queueing : Kuyruk (QoS).
Rate-limiting : Hız sınırlaması.
Rogue : Sahte.
Root bridge : Kök köprü.
Route poisoning : Yönlendirme döngülerini önlemeye yarayan bir mekanizma.
Route redistribution : Routing protokollerinde yol bilgisinin farklı bir metot ile duyurulması.
Routed interface : IP adresi verilebilen L3 ara yüz.
Router : Yönlendirici.
Routing : Yönlendirme.
Routing loop : Yönlendirme döngüsü.
Running-config : Cisco cihazlarda çalışan konfigürasyonun adı.
Server farm : Sunucu kümesi.
Snooping : Bir fonksiyonun yetki alanını aşarak bilgi edinme yöntemi.
Split : Ayrı.
Split horizon : Yönlendirme döngülerini önlemeye yarayan bir teknik.

Spoof	: Aldatmaca.
State	: Durum.
Stateful	: Durumsal, duruma dayalı.
Storm	: Normalden fazla gelen unicast, multicast ve/vaya broadcast trafiği ifade eder.
Subnet mask	: Altağ maskesi.
Summary	: Özet.
Supervisor engine	: Şase tabanlı anahtarlarda cihazı kontrol eden ve L3 yönlendirmeyi yapan modül.
Switch	: Anahtar.
Switching	: Anahtarlama.
Syslog	: Sistem durum kayıtları.
Tail drop	: Paket sıkışması anında sıralı paket atımı.
TCP/IP	: DoD modeline göre üretilmiş protokol ailesine genel olarak verilen isim.
Topology	: Şema, yapı.
Tracking	: İzleme, takip.
Traffic policing	: Trafik politikası (QoS).
Traffic shaping	: Trafik şekillendirme (QoS).
Transform set	: Dönüşüm seti.
Transparent Bridge	: Şeffaf köprü.
Triggered update	: Değişiklik oluştuğu anda zamanlayıcıları beklemeden yapılan güncelleme duyurusu.
Trunk	: Birçok VLAN trafiğini iletebilen anlamında kullanılır.
Trust boundary	: Güven sınırı (QoS).
Trust exploitation	: Güven istismarı (QoS).
Virtual Interface	: Sanal arayüz.
Voice	: Ses.