T.C
ÖLÇME, SEÇME VE YERLEŞTİRME MERKEZİ BAŞKANLIĞI

KAMERA, PARMAK İZİ VE YÜZ TANIMA SİSTEMLERİNİN BİLİŞİM ALTYAPISINA İLİŞKİN TEKNİK ŞARTNAME

İÇİNDEKİLER

1. AMAÇ

ÖSYM bünyesinde bulunan Kamera ve Parmak İzi sistemlerinin yenilenmesi, buna ek olarak Yüz tanıma sisteminin de güvenliği artırıcı bir unsur olarak temin edilmesi planlanmıştır. Kurulması ve yenilenmesi planlanan sistemler için gerekli olan veri depolama sistemi ve ağ cihazlarının temini amaçlanmıştır.

2. KAPSAM

ÖSYM güvenlik sistem altyapısından kullanılması planlanan ve teknik özellikleri aşağıdaki bölümlerde belirtilen donanımları aşağıdaki tabloda belirtilen adetlerde temin edilecektir.

Donanım Adı	Adet
Veri Depolama Sistemi	1
Omurga Anahtar	2
Kenar Anahtar	12
Dış Saha Anahtarları	10

3. GENEL HUSUSLAR

3.1. Yüklenici tarafından teslim edilecek tüm Donanımları oluşturan tüm parçalar yeni ve orijinal olacaktır. Cihaz ve malzemelerin hiç bir bölümünde kırık, çatlak, deformasyon ve malzeme hataları bulunmayacaktır.

3.2. Bu teknik şartname kapsamında kurulacak Donanım ve Yazılım, kullanıcıda bulunan mevcut donanım ve yazılımlarla uyumlu olacak ve sorunsuz çalışması Yüklenici tarafından sağlanacaktır.

3.3. Yazılım ve donanımlarla beraber gelen dokümanlar en az 1 (bir) adet olacak şekilde CD/DVD ortamında İdare'ye teslim edilecektir. Her türlü malzemeye ait dokümanlar bir orijinal (eğer orijinali Türkçe değilse) bir de Türkçe kopya olarak teslim edecektir.

3.4. Yüklenici, Donanımlar'ın kurulum ve kullanımı için gerekli tüm yazılım (firmware) ve sürücü gereksinimlerini eksiksiz sağlayacaktır.

3.5. Montaj esnasında Yüklenici kendi teçhizatı dışında kalan diğer sistem ve teçhizata hasar verdiği takdirde hasardan sorumlu tutulacak ve tüm zararı karşılayacaktır.

3.6. Yüklenici sorumluluğundaki teçhizatın sevkiyatı esnasında meydana gelebilecek her türlü hasar, Yüklenici tarafından karşılanacaktır.

3.7. Tüm sistem ve bağlı donanımlar 220 (iki yüz yirmi) ± 10 (on) VAC, 50 (elli) Hz frekans elektrik özelliklerinde çalışabilecektir.

3.8. Teklif edilecek ürünlerin End of Life (EOL) duyurusu yapılmamış olması gerekmektedir.

3.9. Şartname kapsamında teklif edilen tüm sistemler kendi ürün ailesinin en son jenerasyon ürünü olacaktır.

3.10. Ağ anahtarı üretici firmanın Ankara'da yerleşik bir ofis yapılanması olacaktır.

3.11. Donanımların çalışması için gerekli her türlü bağlantı kablosu, güç kablosu, soket, konnektör, adaptör ve buna benzer donanım Yüklenici tarafından sağlanacaktır.

3.12. Sistemlerin gerekli tüm kablolama ve montaj işlemleri Yüklenici tarafından sağlanacaktır.

4. GARANTİ ve TESLİM ŞARTLARI

4.1. Yüklenici, Sözleşme kapsamında teslim edeceği Donanım ve Yazılımlar için, kesin kabul tarihinden itibaren -yedek parça dahil 5 (beş) yıl mal ve hizmet garantisi verecektir. Yüklenici, tedarikçi/üreticilerinden temin ederek, İdare'ye teslim edeceği Donanım ve Yazılımlar'a ait garanti belgelerini İdare adına düzenletmek ve orijinal nüshalarını İdare'ye teslim etmekle mükelleftir. Alınan Donanım ve Yazılımlar'a ilişkin İdare adına garanti belgesi düzenlenmesinin mümkün olmaması durumunda yüklenici garantiye ilişkin taahhütleri içeren bir belgeyi İdare'ye sunmak zorundadır. Garanti kapsamındaki Donanım ve Yazılımlar'da sözleşme süresi içerisinde tespit edilecek hata, ayıp ve eksikliklerin garanti sağlayan kişi veya kuruluş tarafından giderilmesini Yüklenici üstelenecektir.

4.2. Donanımlar üzerinde çalışan gömülü yazılımların yeni sürümleri ve yamaları garanti süresi içerisinde ücretsiz olarak Yüklenici tarafından sağlanacaktır. Yeni yazılımlar ve yamalar, kullanıma sunulduğu tarihten itibaren en geç 15 (on beş) gün içerisinde Yüklenici tarafından İdare'ye teslim edilecek veya İdare'ye yazılımlara internet üzerinden erişim ve indirme ortamı sağlanacaktır.

4.3. Garanti süresince arızalanan diskler hiçbir şekilde Yüklenici veya üretici firmaya iade edilmeyecektir.

4.4. Yüklenici; Donanım ve Yazılımların garanti süresi içinde, gerek malzeme ve işçilik gerekse montaj hatalarından dolayı arızalanması halinde işçilik masrafı, değiştirilen parça bedeli ya da başka herhangi bir ad altında hiçbir ücret talep etmeksizin tamirini yapmak veya yaptırmakla yükümlüdür.

4.5. Yüklenici, garanti süresi boyunca, malın kullanım kılavuzu veya diğer dokümantasyonunda belirtilen periyotlarda bakımını, her türlü sarf malzemesinin bedeli kendine ait olmak üzere gerçekleştirecektir.

4.6. Malın arızalanması durumunda tamirde geçen süre garanti süresine eklenir.

4.7. Donanımlara ilişkin bir arıza ya da sorun İdare tarafından Yüklenici'ye bildirildiği andan itibaren en geç 4 (Dört) saat içerisinde arıza/soruna müdahale edecektir. Bildirilen arıza/sorun en geç 2 (iki) iş günü içerisinde giderilecektir. Arıza/sorunun giderilememesi halinde Yüklenici tamir sonuna kadar benzer özelliklere sahip başka bir malı İdare'ye tahsis eder. Yüklenici tarafından sağlanacak her türlü sistem ve orijinal yedek parça en az değişen parçanın teknik/fonksiyon özelliklerine sahip olacaktır.

5. TEKNİK ÖZELLİKLER

5.1. VERI DEPOLAMA SİSTEMİ

5.1.1. Veri depolama sistemi en az 2 adet aktif-aktif çalışan kontrol ünitesine sahip olacaktır.

5.1.2. Veri depolama sistemi en az 24 GB DRAM tipinde ön belleğe sahip olacaktır.

5.1.3. Veri depolama sistemi en az 8 adet en az 8 Gb FC bağlantı portu sağlamalıdır.

5.1.4. Veri depolama sistemi (RAID 0,1 veya RAID 10) ve (RAID 5 veya RAID 50) ve RAID 6 koruma yöntemlerini destekleyecektir.

5.1.5. Veri depolama sisteminde en az 5 adet en az 200 GB kapasiteli SSD disk bulunmalıdır.

5.1.6. Veri depolama sistemi en az 3 TB ve en az 7200 rpm diskler ile RAID 6 (en fazla 14+2) koruma yöntemi sonrasında en az 400 TB net kullanılabilir kapasite ile teklif edilmelidir.

5.1.7. Veri depolama sistemi üzerinde hotspare disk/alan tanımlanabilmelidir.

5.1.8. Veri depolama sistemi mekanik diskler için her 24 adet disk için en az 1 adet hotspare disk veya buna karşılık gelen spare alan ile teklif edilmelidir.

5.1.9. Veri depolama sistemi en az 360 adet diske genişletilebilmelidir.

5.1.10. Veri depolama sistemi en az 6 Gb SAS disk bağlantı hızına sahip olmalıdır.

5.1.11. Veri depolama sisteminde tek noktadan hata durumuna karşı önlemler alınmış olmalı ve herhangi bir parçanın arızasında yedek birim sistemin durmadan çalışmasını sağlamalıdır.

5.1.12. Veri depolama sistemi üzerinde bulunan hatalı sistem parçaları(disk, bellek, I/O üniteleri, güç kaynağı, fanlar vb.) sistem çalışırken ve erişim kesintisine sebep olmadan değiştirilebilmelidir.

5.1.13. Veri depolama sisteminin elektrik kesintisinde ön belleğindeki verilerin kaybedilmemesi için pil, akü veya alternatif teknolojiler ile korunması sağlanmalıdır.

5.1.14. Veri depolama sistemi Microsoft Windows Server (2008, 2012), Linux(Red Hat) işletim sistemleri, bu işletim sistemlerinin kümeleme yazılımları ve VMware, Hyper-V ve benzeri sanallaştırma sistemleri ile sorunsuz çalışacaktır.

5.1.15. Veri depolama sistemi grafik ara yüze sahip bir yönetim yazılımı ile yönetilebilmeli, anlık ve geriye dönük performansı izlenebilmeli ve eğer lisans gerekiyorsa teklif edilmelidir.

5.1.16. Veri depolama sistemine erişecek sunucuların ve bu sunucuların kullanacağı mantıksal alanların sayısı ile ilgili lisans kısıtlaması olmamalı, eğer lisans gerekiyorsa desteklediği en yüksek kapasite teklif edilmelidir.

5.1.17. Veri depolama sistemi sunucu bağlantılarının yedekli ve yük dağıtımlı olarak çalışabilmesini sağlamalıdır, eğer lisans gerekiyorsa teklif edilmelidir.

5.1.18. Veri depolama sistemi thin provisioning özelliğini desteklemelidir, eğer lisans gerekiyorsa teklif edilmelidir.

5.1.19. Veri depolama sistemi snapshot ve clone özelliklerini desteklemelidir, eğer lisans gerekiyorsa teklif edilmelidir.

5.1.20. Veri depolama sistemi otomatik veri katmanlama özelliğini desteklemelidir.

5.1.21. Veri depolama sistemi SSD diskleri ön bellek olarak kullanabilme özelliğini desteklemelidir, eğer lisans gerekiyorsa teklif edilmelidir.

5.1.22. Veri depolama sistemi orjinal kabini ile teklif edilecektir.

5.1.23. Veri depolama sistemi ile SAN arasındaki gerekli bağlantı kabloları teklif edilecektir.

5.1.24. Veri depolama sistemi üretici firmanın garanti süresince, iş günlerinde 4 saatte müdahele ve en geç bir sonraki iş günü parça değişimini kapsayan garanti ve destek paketi ile teklif edilecektir.

5.1.25. Veri depolama sistemindeki performans ve yapılandırma problemlerine destek hizmeti verilmelidir.

5.1.26. Veri depolama sistemi destek hizmeti microcode/yazılım güncellemelerini

kapsamalıdır.

5.1.27. Veri depolama sistemi arıza oluşması durumunda otomatik çağrı açabilmeli veya mail atabilmelidir.

5.1.28. Veri depolama sistemi üzerinde bozulan disk iade edilmeyecektir.

5.2. AĞ CİHAZLARI

5.2.1. OMURGA ANAHTARLAR

5.2.1.1. Oluşturulacak olan ağda merkez anahtar görevini yapacak 2 Adet Omurga anahtar sağlanacaktır.

5.2.1.2. Teklif edilecek Omurga anahtarlar ile Kenar anahtarlar aynı marka olacaktır.

5.2.1.3. Anahtarların her biri üzerinde en az 24 adet 1GE SFP portu ve en az 4 adet 10GE SFP+ portu bulunacaktır.

5.2.1.4. Omurga anahtarlar yığın(stack) veya Virtual Chassis yöntemleri kullanılarak tek bir cihazmış gibi yönetilecektir.

5.2.1.5. Her bir omurga anahtarı için 24 adet 1000Base-LX SFP ve 4 adet 10GBase-SR SFP+ transceiver sağlanacaktır.

5.2.1.6. Omurga anahtarlarının yığın olarak çalışması için gereken slot, modül, SFP, kablo ürünlerini tamamı teklif edilecektir. Yığın bağlantının toplam hızı en az 16Gbit/s olacaktır. Yığın yapılırken yukarıda belirtilen sistem portlar kullanılmayacaktır. Cihazın ayrı yığın port desteği olacaktır. Omurga anahtarlar Virtual Chassiss yöntemleri kullanılacaksa bu isterler aranmayacaktır

5.2.1.7. Yığın yapıda konfigüre edilen anahtarlar tek bir cihaz gibi çalışabilmeli ve tek bir IP üzerinden yönetilebilecektir.

5.2.1.8. Yığınlanmış anahtarlar gelen paketlerin yerel anahtarlama ve yönlendirmesini yapabilecek, herhangi bir şekilde paketleri yığın master anahtarına göndermesi gerekmeyecektir. Master anahtar arızalandığında otomatik olarak backup'daki anahtar devreye girecektir.

5.2.1.9. Teklif edilecek anahtarlar static IP yönlendirme, RIPv1, RIPv2, dinamik yönlendirme protokollerini destekleyebilmelidir.Ayrıca Lisans artırımı ile OSPF ve BGP protokollerini destekleyecektir.

5.2.1.10. Anahtarlar IPv6 management ve Routing desteklemelidir.

5.2.1.11. Anahtar en az konfigüre edilebilir 1000 adet VLAN desteğine sahip olmalıdır.

5.2.1.12. Teklif edilecek omurga anahtarlar en fazla 1RU yüksekliğinde olacaktır.

5.2.1.13. Önerilecek cihazın backplane kapasitesi(anahtarlama kapasitesi) en az 176 Gbps, paket iletim kapasitesi en az 130 Mpps (Saniyede 130 milyon paket) olmalıdır.

5.2.1.14. Anahtar en az 20.000 MAC adresini desteklemelidir.

5.2.1.15. Anahtar toplam 11.000 adet rota (route) desteklemelidir.

5.2.1.16. Cihaz istenen tüm fonksiyonları yerine getirmeye uygun bellek konfigürasyonuyla (En az 1024 MB SDRAM/DRAM, 512 MB

FLASH/NVRAM, 3 MB PACKET BUFFER) teklif edilecektir.

5.2.1.17. Anahtar Auto MDI/MDI-X özelliklerine sahip olmalıdır.

5.2.1.18. Cihazdaki tüm portlarında otomatik olarak full-duplex/half-duplex iletişimi destekleyecektir.

5.2.1.19. Anahtarlar her kullanıcı portu için rate limiting desteğine sahip olmalıdır.

5.2.1.20. Anahtarlar IEEE 802.3ad Link Aggregation standardını desteklemeli LAG(Link Aggregation Group) oluşturulabilmeli ve her bir grupta en az 8 adet port bulunabilmelidir.

5.2.1.21. Teklif edilen ve tek cihaz gibi çalışmayı destekleyen omurga cihazları, farklı anahtarlar üzerindeki portları bir link grubu içerisinde toplayabilmeli böylece hem yük paylaşımı hem de yedeklilik üst seviyeye çıkarılabilmelidir.

5.2.1.22. Anahtar, IEEE 802.1d Spanning Tree, IEEE 802.1s Multiple Spanning Tree ve IEEE 802.1w Rapid Reconvergence desteklenmelidir. Anahtar Spanning-tree Root, Loop ve BPDU protection özelliklerine sahip olacaktır.

5.2.1.23. Önerilecek cihaz ikinci katmanda yük paylaşımı ve yedeklilik sağlayabilmek için IEEE – 802.1S (MSTP – Multiple Spanning Tree Protocl) desteğini verebilmelidir.

5.2.1.24. Anahtar PVST veya MSTP protokollerini destekleyecektir.

5.2.1.25. Anahtarlar ağ güvenliğini sağlamak amacıyla, ağa bağlanan kullanıcıların yetkilendirilmesi için IEEE 802.1X Port Güvenlik standardını desteklemeli ve RADIUS desteğine sahip olmalıdır.

5.2.1.26. Anahtar 802.1X desteğine sahip olmayan kullanıcıların da ağa bağlanabilmeleri için MAC Adres veya web tabanlı authentication desteklenmelidir.

5.2.1.27. Anahtar birden fazla kullanıcının aynı port üzerinde kimlik doğrulaması ile çalışabilmesi sağlanabilmelidir (multiple-hosts veya multiple-authentication).

5.2.1.28. Anahtara yönetim erişimi için Radius ve TACACS+ ya da HWTACACS protokolleri desteklenecektir. AAA yapısı içinde anahtar yöneticilerinin erişimi kontrol edilebilecek, girebilecekleri komutlar sınırlandırılabilecektir.

5.2.1.29. Teklif edilen ürün IPv4/IPv6 DHCP client / relay / server desteğine sahip olmalıdır.

5.2.1.30. Anahtarlar WEB tabanlı veya Graphical User Interface(GUI) tabanlı yazılım ile yönetilebilmelidir. Bu yönetimler için ek ücret talep edilmemelidir.

5.2.1.31. Anahtarlara Console port, SNMP V1/v2/v3, SSHv2 (secure shell) ve Telnet üzerinden yönetilebilmelidir. Cihaz endüstri standardı olan CLI (Command Line Interface) özelliğine sahip olacaktır.

5.2.1.32. Anahtarın erişiminde farklı seviyelerde yetkiler tanımlanabilecektir.

5.2.1.33. Anahtar konfigürasyonu flash bellekte tutulacaktır. Anahtarlar üzerinde birden fazla konfigürasyon dosyası muhafaza edilebilmelidir.

5.2.1.34. Anahtarlar Port mirroring desteğine sahip olmalıdır. Birden fazla kaynak port bir porta mirror edilebileceği gibi birden fazla kaynak port'da seçilebilmelidir. Anahtar farklı anahtarlardaki kaynak port ve VLAN'ları dinleyebilmek için remote-mirroring destekleyecektir.

5.2.1.35. Anahtarın log bilgisi harici bir Syslog sunucuya gerçek zamanlı olarak aktarılabilmelidir.

5.2.1.36. Anahtarın sFlow veya Netflow desteği bulunacak.

5.2.1.37. Teklif edilecek olan anahtarın kendine direkt bağlı cihazları öğrenme özelliği (neighbor learning) olmalıdır.

5.2.1.38. Anahtarlar güncel Firmware yazılımı ile teklif edilmelidir.

5.2.1.39. Anahtarlar IEEE 802.1Q VLAN standartlarını desteklemelidir.

5.2.1.40. Anahtarlar DHCP Snooping, DAI(Dynamic ARP Inspection) ve IP Source Guard güvenlik özelliklerini desteklemelidir.

5.2.1.41. Üçüncü seviyede (L3) DiffServ Code Point (DSCP) ya da ikinci seviyede (L2) IEEE 802.1p CoS (Class of Service) ile sınıflandırılmış paketlerin öncelik değerlerini anlayabilmeli, gerektiğinde bu öncelik değerlerini değiştirebilmelidir.

5.2.1.42. Anahtar, paketleri L2 başlığındaki kaynak/hedef MAC adresi, L3 başlığındaki kaynak/hedef IP adresi, L4 başlığındaki TCP/UDP port numarası bilgilerine göre erişim denetiminden geçirebilmelidir.

5.2.1.43. Erişim kontrol filtreleri/listeleri zamana bağlı devreye girecek şekilde kullanılabilecektir.

5.2.1.44. Anahtar üzerinde bulunan portlar için MAC adresi bazında kullanıcı listeleri oluşturulabilmeli ve böylece port güvenliği sağlanabilmelidir.

5.2.1.45. Anahtarlar multicast veri trafiğinin sadece talep edilen sistemlerden alınmasını sağlayarak ağın ve son kullanıcı sistemlerinin performansını korumalıdır.

5.2.1.46. Anahtarlar oluşabilecek Broadcast ve Multicast Stormları engelleyebilecek, IGMP Multicast Filtering ve Snoopingdestekleyecektir. Anahtarlar IGMP v1, IGMPv2 ve IGMP v3 ve IGMPv1/v2/v3 Snooping desteğine sahip olacaktır.

5.2.1.47. Anahtar istendiğinde yazılım arttırımı ile PIM sparse mode (PIM-SM), PIM dense mode (PIM-DM), PIM sparse-dense mode ve Source Specific Multicast (SSM) protokollerini destekleyebilmelidir.

5.2.1.48. Anahtarlar VRRP veya HSRP desteğine sahip olmalıdır.

5.2.1.49. Anahtarlar en az 9.000 byte jumbo frame desteğine sahip olmalıdır.

5.2.1.50. Anahtarlar 19 inch standart kabinlere monte edilebilir olmalıdır ve Kabine montaj elemanları ile birlikte verilmelidir.

5.2.1.51. Teklif edilen cihaz, 220V ve 50Hz şebeke gerilimi ile beslenmelidir. Güç kabloları Türkiye şartlarına uygun olmalıdır.

5.2.1.52. Teklif edilen cihazlar yedekli güç kaynağına sahip olacaktır.

5.2.2. KENAR ANAHTARLAR

5.2.2.1. Oluşturulacak ağda erişim anahtar görevini yapacak 12 adet kenar

anahtar sağlanacaktır.

5.2.2.2. Teklif edilecek Kenar anahtarlar ile Omurga anahtarlar aynı marka olacaktır.

5.2.2.3. Teklif edilecek Kenar Anahtarların 10 tanesinin üzerinde en az 48 adet10/100/1000 Mbps RJ-45 port bulunacaktır. Bu portlardan en az 4 tanesine 1000 Base-X fiber bağlanabilmeli ya da bu portların dışında 4 tanesine 1000 Base-X fiber portu bulunmalıdır.

5.2.2.4. Teklif edilecek Kenar Anahtarların 2 tanesinin üzerinde en az 24 adet10/100/1000 Mbps RJ-45 Base-TX port bulunacaktır. Bu bu portların dışında 4 tanesine 1000 Base-X fiber portu bulunmalıdır.

5.2.2.5. Kenar Anahtarlar için toplamda 24 adet 1000Base-LX SFP transceiver sağlanacaktır.

5.2.2.6. Teklif edilecek 48 portlu anahtarların 6 tanesi kullanılarak 3 adet farklı stack yapısı oluşturulacaktır. Bu kapsamda belirtilen sayıdaki kenar anahtarlarının yığın olarak çalışması için gereken slot modüle, kablo ürünlerini tamamı teklif edilecektir. Yığın bağlantının toplam hızı en az 8Gbit/s olacaktır.

5.2.2.7. Yığın yapıda konfigüre edilen anahtarlar tek bir cihaz gibi çalışabilmeli ve tek bir IP üzerinden yönetilebilecektir.

5.2.2.8. Yığınlanmış anahtarlar gelen paketlerin yerel anahtarlama ve yönlendirmesini yapabilecek, herhangi bir şekilde paketleri yığın master anahtarına göndermesi gerekmeyecektir. Master anahtar arızalandığında otomatik olarak backup'daki anahtar devreye girecektir.

5.2.2.9. Teklif edilecek anahtarlar statik IP yönlendirmeyi destekleyen yazılım ve donanım değerleri ile birlikte teklif edilmelidir.

5.2.2.10. Anahtarlar IPv6 management, Routing yapılarını desteklemelidir.

5.2.2.11. Anahtar en az konfigüre edilebilir 250 adet VLAN desteğine sahip olmalıdır.

5.2.2.12. Teklif edilecek omurga anahtarlar en fazla 1RU yüksekliğinde olacaktır.

5.2.2.13. Önerilecek cihazın backplane kapasitesi(anahtarlama kapasitesi) en az 100 Gbps, paket iletim kapasitesi en az 70 Mpps (Saniyede 70 milyon paket) olmalıdır.

5.2.2.14. Anahtar en az 8.000 MAC adresini desteklemelidir.

5.2.2.15. Anahtar istenen tüm fonksiyonları yerine getirmeye uygun bellek konfigürasyonuyla (128 MB RAM ve 16 MB Flash) teklif edilecektir.

5.2.2.16. Anahtar Auto MDI/MDI-X özelliklerine sahip olmalıdır.

5.2.2.17. Cihazdaki tüm portlarında otomatik olarak full-duplex/half-duplex iletişimi destekleyecektir.

5.2.2.18. Anahtarlar her kullanıcı portu için rate limiting desteğine sahip olmalıdır.

5.2.2.19. Anahtarlar IEEE 802.3ad Link Aggregation standardını desteklemeli LAG(Link Aggregation Group) oluşturulabilmeli ve her bir grupta en az 8 adet port bulunabilmelidir.

5.2.2.20. Anahtar, IEEE 802.1d Spanning Tree, IEEE 802.1s Multiple Spanning Tree ve IEEE 802.1w Rapid Reconvergence desteklenmelidir. Anahtar Spanning-tree Root, Loop ve BPDU protection özelliklerine sahip olacaktır.

5.2.2.21. Önerilecek cihaz ikinci katmanda yük paylaşımı ve yedeklilik sağlayabilmek için IEEE – 802.1S (MSTP – Multiple Spanning Tree Protocl) desteğini verebilmelidir.

5.2.2.22. Anahtar PVST veya MSTP yada en az 16 VLAN için ayrı bir Spanning-tree instance'ı çalıştırabilecek bir protokol destekleyecektir.

5.2.2.23. Anahtarlar ağ güvenliğini sağlamak amacıyla, ağa bağlanan kullanıcıların yetkilendirilmesi için IEEE 802.1X Port Güvenlik standardını desteklemeli ve RADIUS desteğine sahip olmalıdır.

5.2.2.24. Anahtar 802.1X desteğine sahip olmayan kullanıcıların da ağa bağlanabilmeleri için MAC Adres veya web-based authentication desteklenmelidir.

5.2.2.25. Anahtar birden fazla kullanıcının aynı port üzerinde kimlik doğrulaması ile çalışabilmesi sağlanabilmelidir (multiple-hosts veya multiple-authentication).

5.2.2.26. Anahtara yönetim erişimi için Radius , TACACS+ yada HWTACACS protokolleri desteklenecektir. AAA yapısı içinde anahtar yöneticilerinin erişimi kontrol edilebilecek, girebilecekleri komutlar sınırlandırılabilecektir. Ayrıca anahtarlarda DHCP Relay desteği olmalıdır.

5.2.2.27. Anahtarlar WEB tabanlı veya Graphical User Interface(GUI) tabanlı yazılım ile yönetilebilmelidir. Bu yönetimler için ek ücret talep edilmemelidir.

5.2.2.28. Anahtarlara Console port, SNMP V1/v2/v3, SSHv2 (secure shell) ve Telnet üzerinden yönetilebilmelidir. Cihaz endüstri standardı olan CLI (Command Line Interface) özelliğine sahip olacaktır.

5.2.2.29. Anahtarın erişiminde farklı seviyelerde yetkiler tanımlanabilecektir.

5.2.2.30. Anahtar konfigürasyonu flash bellekte tutulacaktır. Anahtarlar üzerinde birden fazla konfigürasyon dosyası muhafaza edilebilmelidir.

5.2.2.31. Cihaz Traffic Mirroring özelliğine sahip olmalıdır.

5.2.2.32. Anahtarın log bilgisi harici bir Syslog sunucuya gerçek zamanlı olarak aktarılabilmelidir.

5.2.2.33. Anahtarın sFlow,Netflow veya Netflow-Lite desteği bulunacaktır.

5.2.2.34. Teklif edilecek olan anahtarın kendine direkt bağlı cihazları öğrenme özelliği (neighbor learning) olmalıdır.

5.2.2.35. Anahtarlar güncel Firmware yazılımı ile teklif edilmelidir.

5.2.2.36. Anahtarlar IEEE 802.1Q VLAN standartlarını desteklemelidir.

5.2.2.37. Anahtarlar DHCP Snooping, DAI(Dynamic ARP Inspection) ve IP Source Guard güvenlik özelliklerini desteklemelidir.

5.2.2.38. Üçüncü seviyede (L3) DiffServ Code Point (DSCP) ya da ikinci seviyede (L2) IEEE 802.1p CoS (Class of Service) ile sınıflandırılmış paketlerin öncelik değerlerini anlayabilmeli, gerektiğinde bu öncelik değerlerini değiştirebilmelidir.

5.2.2.39. Anahtar, paketleri L2 başlığındaki kaynak/hedef MAC adresi, L3 başlığındaki kaynak/hedef IP adresi, L4 başlığındaki TCP/UDP port numarası bilgilerine göre erişim denetiminden geçirebilmelidir.

5.2.2.40. Erişim kontrol filtreleri/listeleri zamana bağlı devreye girecek şekilde kullanılabilecektir.

5.2.2.41. Anahtar üzerinde bulunan portlar için MAC adresi bazında kullanıcı listeleri oluşturulabilmeli ve böylece port güvenliği sağlanabilmelidir.

5.2.2.42. Anahtarın multicast desteği olmalı ve Snooping desteklemelidir. Ayrıca anahtar IEEE 802.3x özelliğini desteklemelidir.

5.2.2.43. Anahtarlar en az 9.216 byte jumbo frame desteğine sahip olmalıdır.

5.2.2.44. Anahtarlar 19 inch standart kabinlere monte edilebilir olmalıdır ve Kabine montaj elemanları ile birlikte verilmelidir.

5.2.2.45. Önerilecek cihaz, 220V ve 50Hz şebeke gerilimi ile beslenmelidir. Güç kabloları Türkiye şartlarına uygun olmalıdır.

5.2.2.46. Anahtarlar üzerinde bulunan tüm 10/100/1000BASE – T / TX portlar üzerinden 802.3af PoE(Power Over Ethernet) ve 802.3at PoE+(Power Over Ethernet Plus) standartlarına uygun olarak enerji verilebilmelidir.

5.2.3. DIŞ SAHA ANAHTARLARI

5.2.3.1. Cihaz üzerinde en az 12 adet 10/100 BaseT ve 2 adet 1000Base-X port bulunacaktır.

5.2.3.2. En az 8,000 adet MAC adres desteklenecektir.

5.2.3.3. Cihaz IEEE 802.3ad Link Aggregation desteklemelidir.

5.2.3.4. Önerilen cihaz tam yedekli bir network altyapısı için gerekli olan Rapid STP desteği bulunmalıdır. Bu sayede network converge time minimize edilerek cihaz ve alt yapı problemlerinde networkun uygulamalar etkilemeden çalışmasına olanak sağlanmış olacaktır.(IEEE 802.1w). Yedekliliğin yanında yük paylaşımının da sağlanabilmesi MSTP (IEEE 802.1s) protokollerini de desteklenmelidir.

5.2.3.5. Cihaz istenen tüm fonksiyonları yerine getirmeye uygun bellek konfigürasyonuyla teklif edilecektir.

5.2.3.6. Cihazdaki tüm portlarında otomatik olarak full-duplex/half-duplex iletişimi destekleyecektir.

5.2.3.7. Anahtar, SNMP v1, v2 ve v3 destegine sahip olmalidir. Cihaz telnet, SSHv2, konsol port araciligi yönetilebilmelidir. Web browser SSL(HTTPS), tabanlı yönetim desteklenecektir.

5.2.3.8. Cihazın üzerinde en son ve en gelişkin özelliklere sahip Firmware ile teklif edilmelidir.

5.2.3.9. Network üzerindeki Multicast trafiklerinin kontrol altında tutulabilmesi amacı ile IGMP snooping ve IGMP filtering desteklemelidir.

5.2.3.10. Cihaz üzerinde erişim kontrol filtreleri/listeleri tanımlanabilmelidir

5.2.3.11. Cihaz Radius tabanlı IEEE 802.1x network login özelliğine sahip olmalıdır. Ayrıca güvenlik amaçlı olarak istendiğinde port başına MAC bazlı erişim kontrolü yapılabilmelidir.

5.2.3.12. 802.1x ve MAC authentication birlikte kullanılabilmeli burada kullanıcı hem 802.1x hem de MAC authentication'dan geçmek zorunda bırakılabileceği gibi 802.1x veya MAC authentication'dan birinden geçtiğinde ağa erişimi kabul edilebilmelidir.

5.2.3.13. Anahtar RMON desteği aracılığıyla istatistiki bilgiler, alarmlar, ve diger bilgiler sorgulanabilmelidir ve RFC2819 veya RFC1757 Group 1,2,3 & 9 özellikleri desteklenecektir.

5.2.3.14. Cihaz kendisine direkt bağlı diğer anahtarları öğrenebilme özelliğine sahip olacaktır.

5.2.3.15. Anahtar montaj parçaları ile birlikte teklif edilecektir.

5.2.3.16. Anahtarlar üzerinde bulunan tüm 10/100/1000BASE – T / TX portlar üzerinden 802.3af PoE(Power Over Ethernet) ve 802.3at PoE+(Power Over Ethernet Plus) standartlarına uygun olarak enerji verilebilmelidir.

5.2.3.17. Anahtarların -10C ve +50C derece arasında çalışacağını yüklenici taahhüt edecektir.

5.2.3.18. Anahtarlar, iadrede bulunan 600mmx360mmx700mm (WxDxH) boyutlarına sahip saha dolaplarına uyacak şekilde olacaktır.

Bu şartname toplam 12 (on iki) sayfadır.