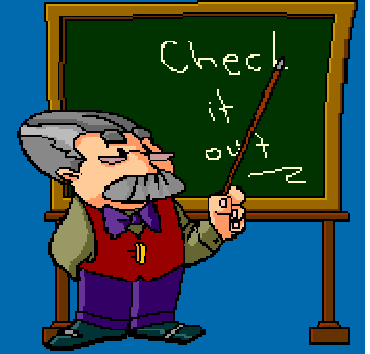


Kampüs Ağ Yönetimi

Ar. Gör. Enis Karaarslan
Ege Ü. Kampüs Network Yöneticisi

Ege Üniversitesi BİTAM
Kampüs Network Yönetim Grubu

İÇERİK



1. Kampüs Ağları
2. Fiziksel Altyapının Sağlıklı Çalışmasının Sağlanması
3. Kampüs Ağının Tanımlanması
4. Ağ Yönetimi
5. Ağ Güvenliğinin Sağlanması
6. Ağ Tabanlı Servislerin Yönetimi
7. Kullanıcıların Bilinçlendirilmesi

1. Kampüs Ağları

Farklı binalara yayılmış farklı yerel ağları (LAN) birleştiren büyük ağlardır

➤ Kampüs Ağlarının kompleksliği

- Çok sayıda bilgisayar
- Çok sayıda iletişim cihazından (hub, switch, router... vb)
- Sanal Ağlar (VLAN)

Kampüs Ağları(devam)

- Ağın büyüklüğü yönetilmesini zorlaştırmaktadır
- Kampüs ağlarının düzgün çalışmasının sağlanması için yapılması gerekenler ...

2.Fiziksel Altyapı

➤ Elektrik altyapısı

- Adanmış sigortalardan hat
- Topraklama
- UPS
- Jeneratör

➤ Yapısal Kablolama

- Kaliteli malzeme (ISO 9000)
- EIA/TIA-568B

2.Fiziksel Altyapı (devam)

- Fiber hattın sağlam kalması
 - Binalar arası Zırhlı Outdoor kablo
 - Bilgili ve ilgili Yapı İşleri
 - Kepçe-savar
- Düşmanlar : Toz / Sıcak
 - Kabinet, kompresör ...

3.Kampüs Ağının Tanımlanması

- Ağ Topolojisi Çizimleri
- Alt ağlar (subnet) - VLAN
- Bilgisayar sayısı – Aktif PC
- Band genişliği (bandwidth)
- Bağlantı (connection) sayısı

3.Kampüs Ağıının Tanımlanması (devam)

- Trafiğin cinsi – İstenmeyen trafik?
- Kampüs kaynaklarına erişim yöntemleri –
Kampüs dışından, Kampüs içi wireless
- Servis sağlayan sunucu makineleri
- Kullanıcı Profili

4.Ağ Yönetimi

- SNMP tabanlı cihaz/hat kontrolü
- Hattın dinlenmesi (sniff) ve analizi
- Ağ yönetim Sistemleri
(Ciscoverks, HP Openview, Tivoli Netview, CA Unicenter ..vb)

Cihazların Uzaktan Yönetimi

- Bütün ağın topolojisinin çıkartılması,
- Yönetilebilir cihazların yazılım versiyonlarının tespiti ve güncellemesi,
- Konfigürasyon yönetimi,
- Hangi cihazlarda sorun yaşandığının tespiti,
- Performans takibi.

5.Ađ Güvenliđinin Sađlanması

- Risk analizi alıřması
- Güvenlik ve kabul edilebilir kullanım politikasının oluřturulması
- Güvenlik önlemlerinin alınması

5.1.Risk Analizi

- Kurum için maddi-manevi deęer taşıyan sistemler belirlenir
- Bu sistemlerin birim zaman/yıllık işlevlerini görememeleri durumunda yaşanacak kayıp hesaplanır
- Tehditler için önlem projeleri hazırlanır

5.2.Güvenlik Politikası

- Kurumun güvenlik stratejisini tanımlar
- Güvenliğin nasıl ayarlanacağını ve yönetileceğini belirten güvenlik kurallardır
- Teknik kılavuzlar değildir,
- Herkesin anlayacağı basit bir şekilde güvenlik hedeflerini belirlerler.
- Yazılıdır / resmidir

Kullanım Politikası

- Kabul edilebilir kullanım politikası (acceptable use policy)
- Ağ ve bilgisayar olanakların kullanımını konusunda kullanıcıların hakları ve sorumlulukları belirtilir.

5.3. Güvenlik Önlemlerinin Alınması

➤ Güncel Güvenlik Tehditleri takip edilmelidir

➤ Kullanılabilecek kaynaklar:

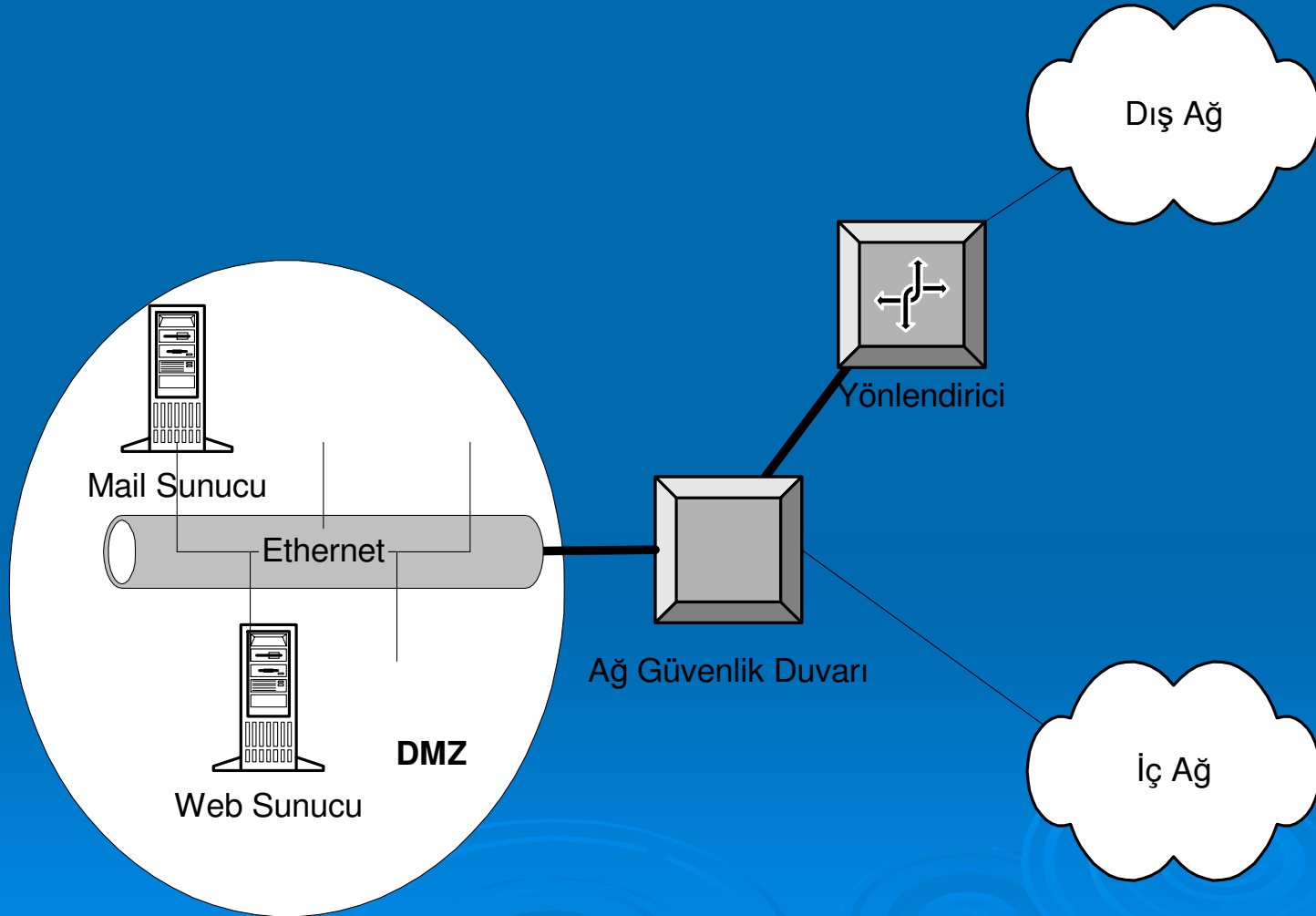
<http://bornova.ege.edu.tr/~enis/guvenlik/>

<http://csirt.ulakbim.gov.tr>

5.3.Güvenlik Önlemlerinin Alınması(devam)

- Aktif Cihazların Güvenliği
- Ağ Güvenlik Duvarı
- Saldırı Tespit Sistemi
- Ağ Tabanlı Antivirüs Sistemleri
- VPN
- Yama Yönetimi

Tipik Bir Ağ

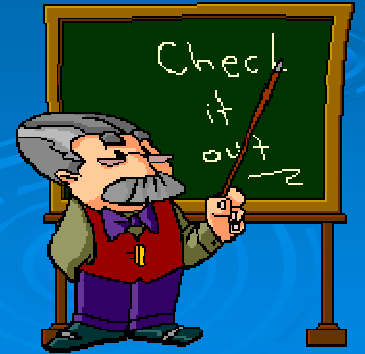


6.Ağ Tabanlı Servislerin Yönetimi

- DNS, DHCP, Web, Mail gibi ağ tabanlı servislerinin düzgün çalışması sağlanmalı
- Yedekleme yapılmalı
- Mail sunucularında relay / spam kontrolü

7.Kullanıcıların Bilinçlendirilmesi

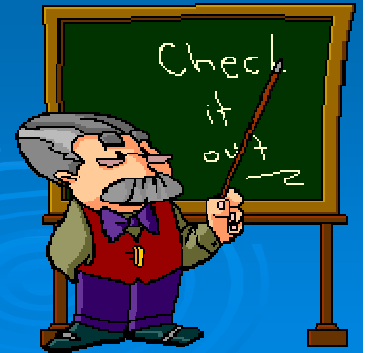
- Kullanıcıların kullandıkları sistemde neyi nasıl yapmaları gerektiği hakkında bilinçlendirilmesi
- Belki de en zor süreç ...
- Eğitim şart ...



7.Kullanıcıların Bilinçlendirilmesi (devam)

➤ Yöntemler:

- Resmi Yazı
- E-posta
- Web portal
(Örn: <http://internet.ege.edu.tr>)
- Seminerler?
- Bilgi yarışmaları?
- Dua ... vb



8.Karşılaşılan Sorunlar

- Elektrik Sorunları
- Toz ve fiziksel erişim
- Virüs
- İstenmeyen trafik
- DHCP / Yanlış Wireless Kurulumları

Çözüm

Standartlara ve Kurallara Uygun Ağ Kullanımı / Yönetimi

SONUÇ

- Bu çalışmada kampüs ağ yönetiminde dikkat edilmesi gerekenler özetlenmiştir.
- Güvenlik ve ağ sorunları hep olacaktır, zaten **ağ yöneticileri (*problem çözücü*)** oluşan sorunları çözmek ve ağın düzgün olarak işlemesini sağlamak için vardır.

SONUÇ (Devam)

- Güvenlik konusunda güncel bilgiler sürekli olarak takip edilmeli ve sorunlar büyümeden gerekli önlemleri alınmalıdır.
- Ağ yönetiminde, standartlara uyulması durumunda mümkün olan en az sorunla yönetilebilecektir.
- Diğer küçük ağlarda da benzer süreçler daha küçük çaplı olarak geçerlidir.

İlginiz için teşekkürler
Sorularınızı bekliyorum.

<http://bornova.ege.edu.tr/~enis>

İletişim için:

enis.karaarslan@ege.edu.tr

Ege Üniversitesi Kampüs Network Yöneticisi