

Säker IP telefoni ?

Hakan Nohre, CISSP

hnohre@cisco.com

Not : Olika former av IP telefoni

Cisco.com

- **Företagets IP telefoni , IP PBX**
- **IP telefoni som operatörstjänst**
- **Internet telefoni**

- **Hårda telefoner**
- **Mjuka telefoner**

Data och Telefoni konvergerar

Hotbilden :

Cisco.com

- **IP Telefoni (VoIP) ärver den hotbild som idag finns mot data applikationer**
 - serversystemen kan attackeras**
 - klienterna (telefonerna) kan attackeras**
 - nätverket kan attackeras**
 - människan kan attackeras**

Data och Telefoni konvergerar

Säkerheten :

Cisco.com

- Vi skyddar ip telefoni med samma metoder som vi skyddar viktiga applikationer (internet banken, sjukjournaler, försvarshemligheter, nästa kvartalsrapport.....)

Det finns andra kritiska applikationer än telefoni, vissa kanske t o m mer kritiska !

Attack mot Serversystemen (Callcontrol, Management)

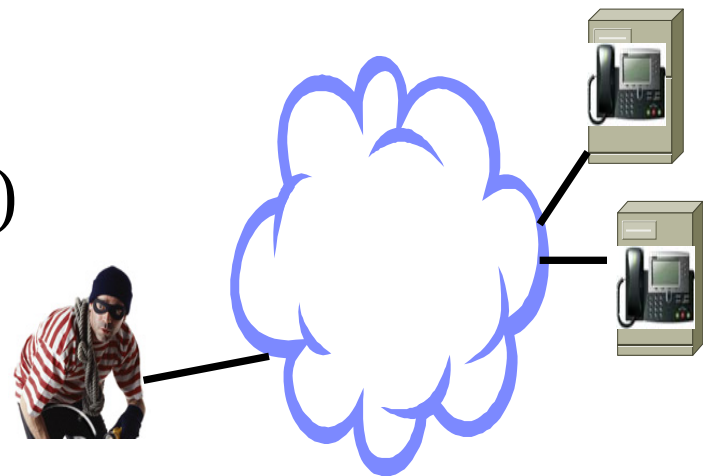
Cisco.com

Attackeras med :

Bug (t.e.x buffertöverskridning)

Dåligt lösenord

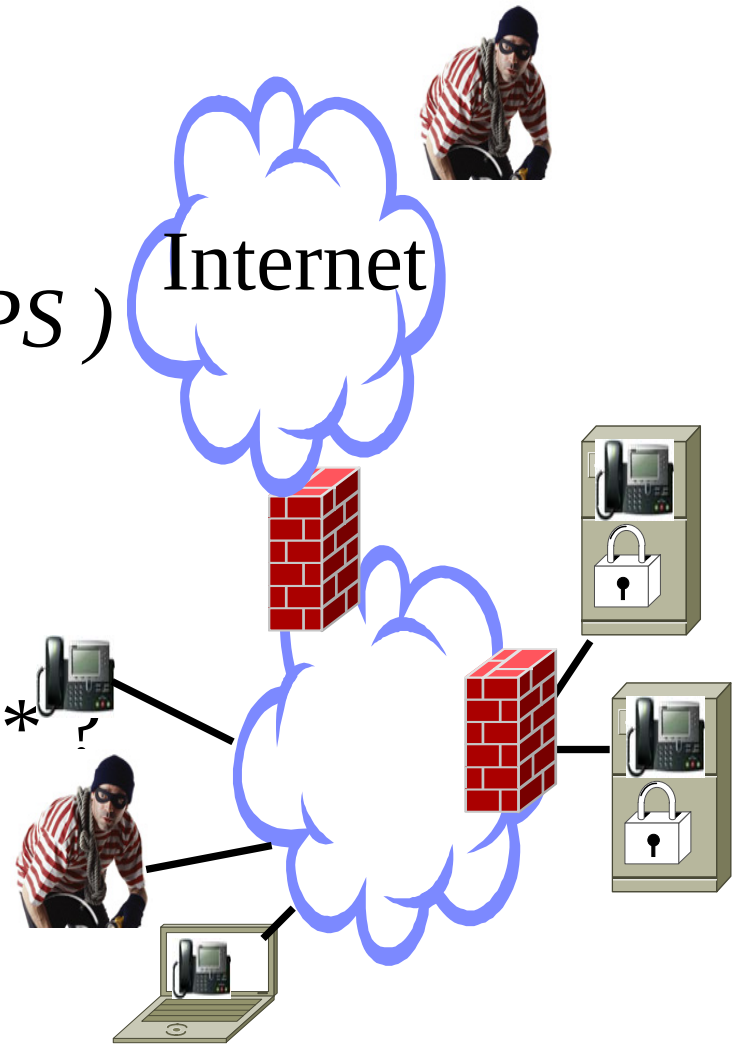
DOS (Belastningsattack)



Skydd av Serversystemen

Cisco.com

Skydda servern
(*uppdaterade patchar, host IPS*)
Brandvägg/IPS*
QoS (rate-limit)
Log analys
Logisk Separation Voice/Data*



Not : Brandväggar och ip telefoni

Cisco.com

IP telefoni är en ”svår” applikation
för brandväggar , dynamiska portar
måste öppnas för talströmmar....

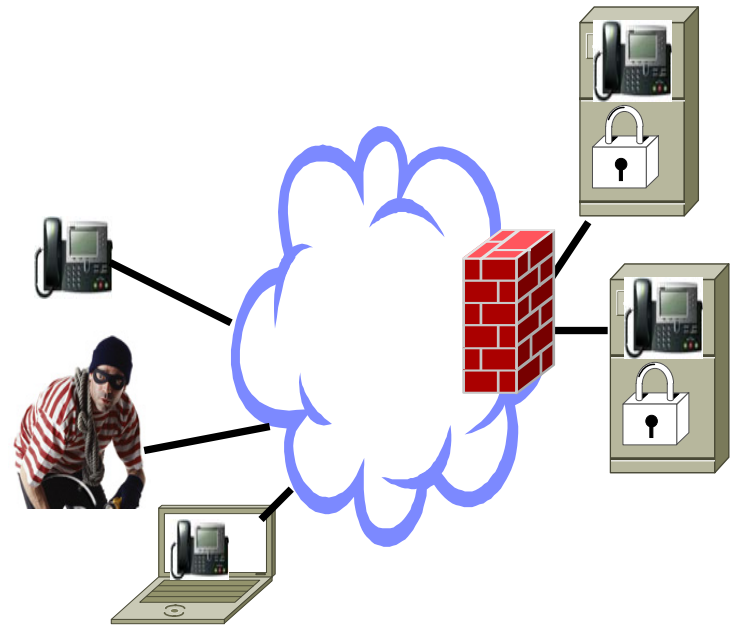
Kräver att brandväggen förstår
ip telefoni protokollet :

H.323vX , H.225, ...

SIP

MGCP

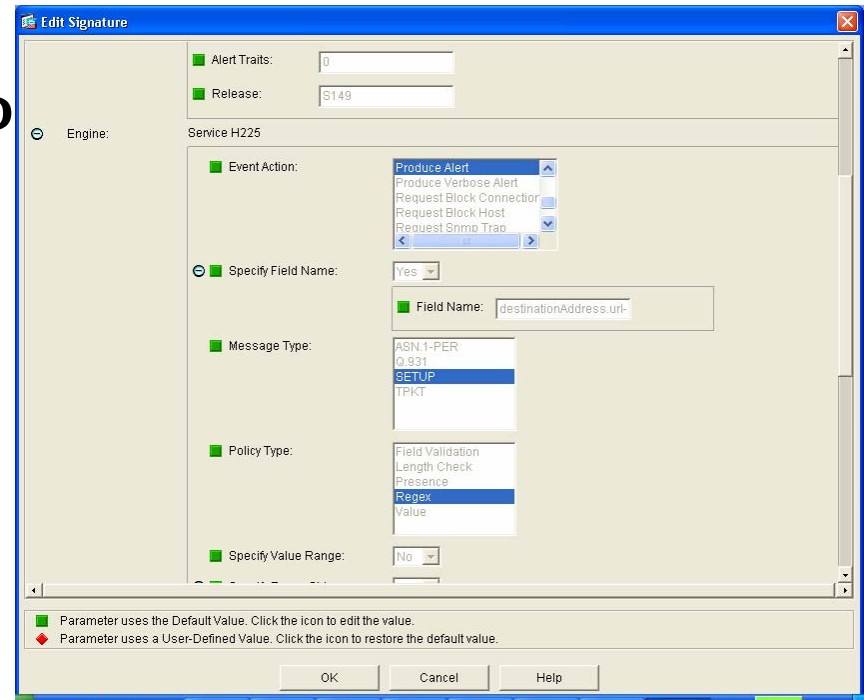
SCCP



Not : Brandväggar och IPS

Cisco.com

De flesta IPS system fokuserar på HTTP, SMTP FTP och vanliga internetprotokoll.



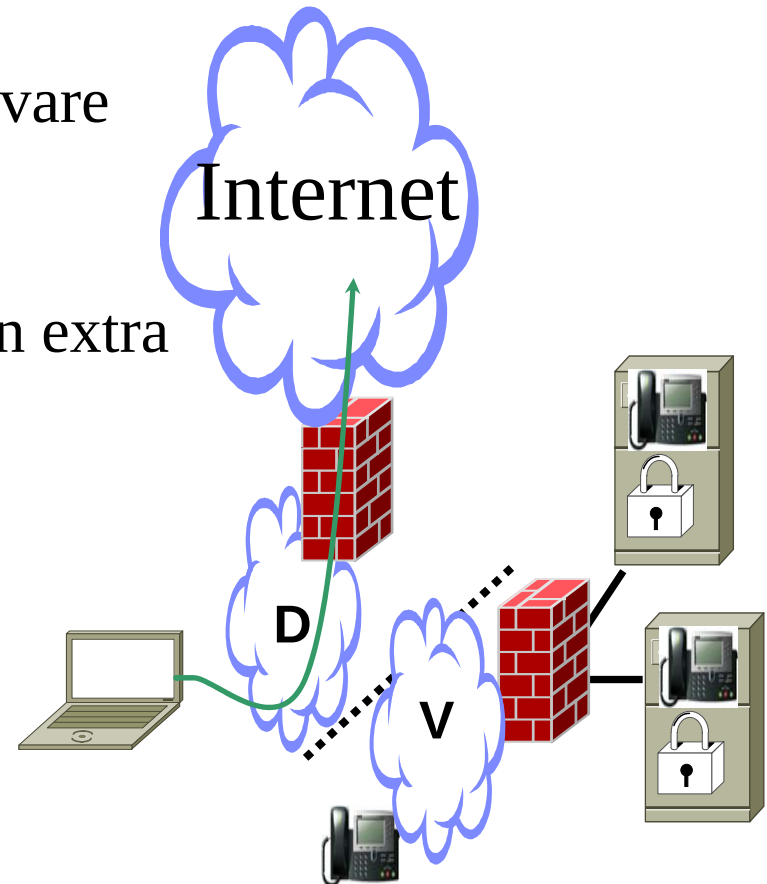
Logisk Separation av tal/data ?

IP telefoner på separat VLAN
(tanken är att datorer ej ges åtkomst till vare sig ip telefoner eller ip telefoni servrar)

Not : Samma fysiska infrastruktur, ingen extra kostnad

Enkelt, Säkert

Soft phones ?



Attack mot Nätverket – sniffning

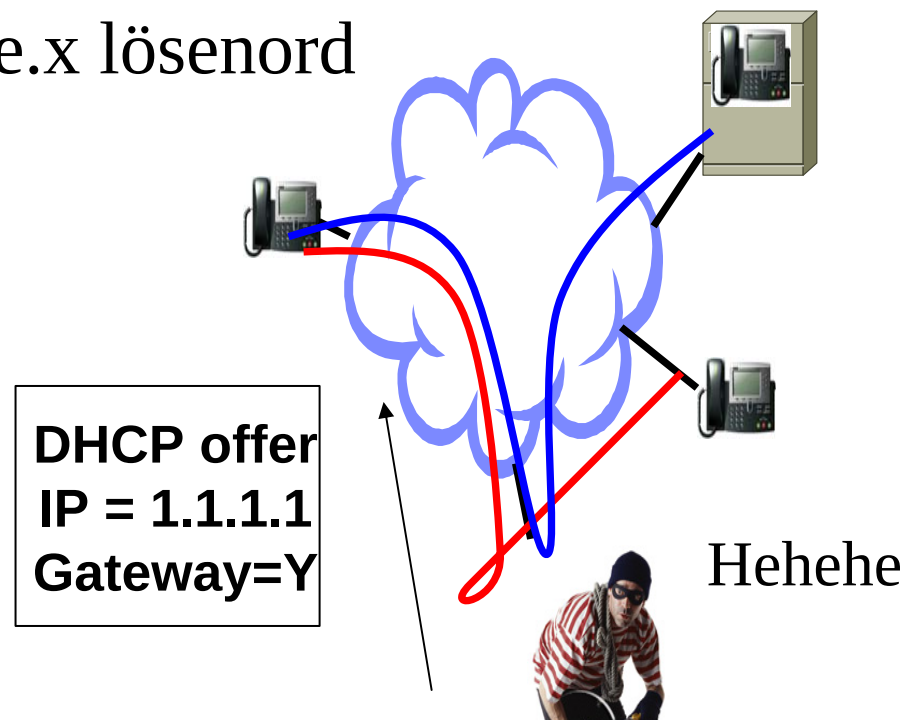
Cisco.com

Avleda* trafiken för att avlyssna

- signaleringen , lära sig t.e.x lösenord
- själva telefonsamtalet

Exempel : Vomit

- * Avledning kan ske genom t.e.x
- ARP spoofing
 - DNS spoofing
 - DHCP spoofing
 - SIP redirect

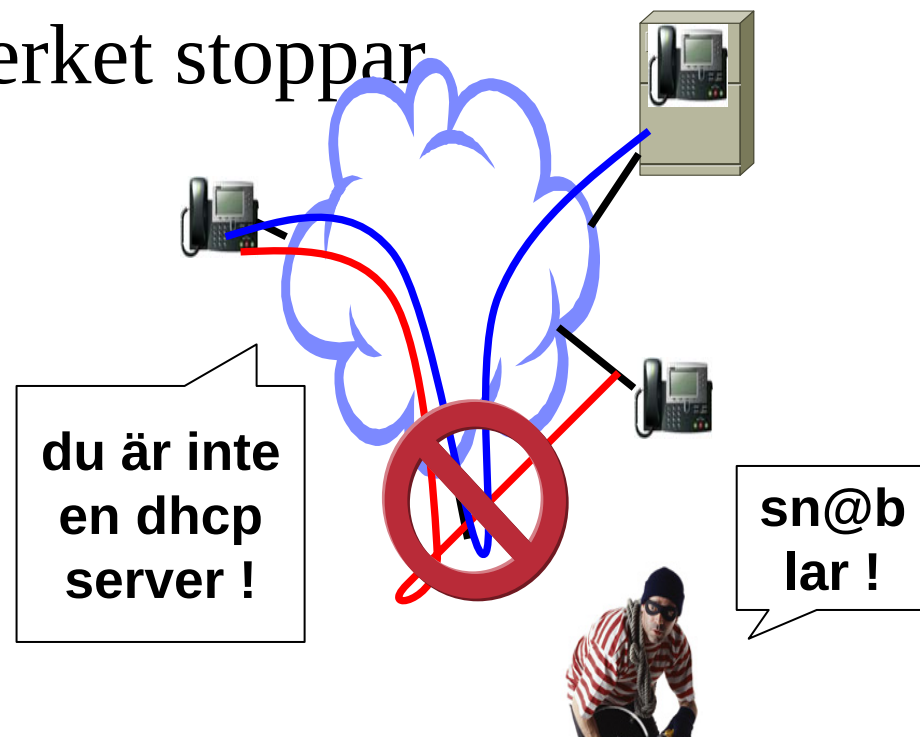


Skydd mot avlyssning – (1)

Cisco.com

Korrekt konfigurerade
säkerhetsfunktioner i nätverket stoppar
avledning av trafik

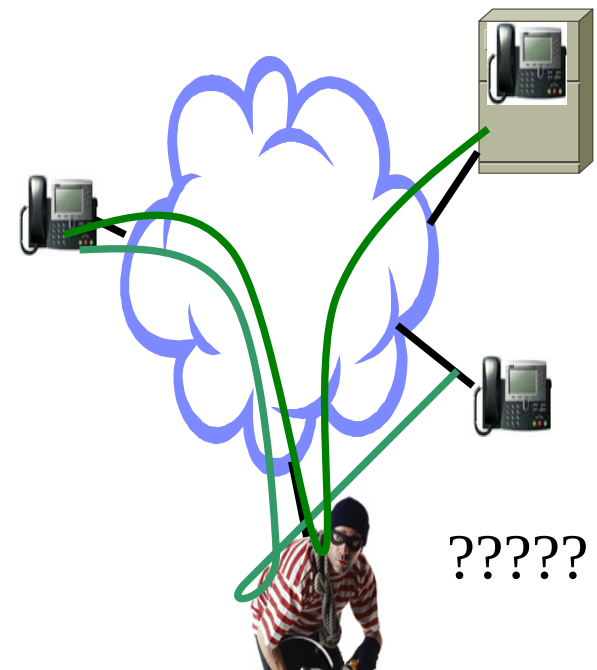
- stoppar ARP spoofing
- stoppar DHCP spoofing



Skydd mot avlyssning– (2)

Cisco.com

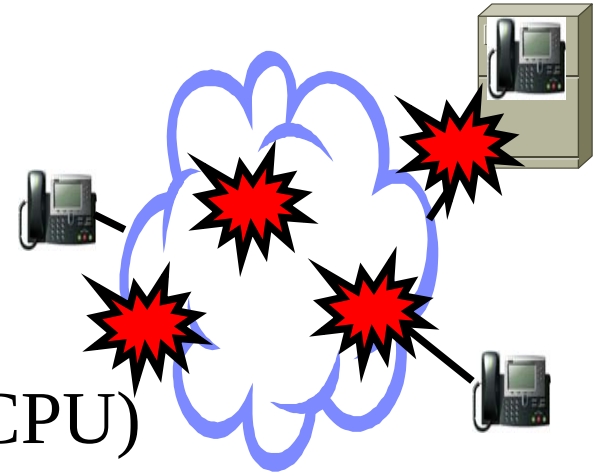
Kryptera
management/signalering
taltrafiken (SRTP)



Överbelastning

Överbelastning

- DOS, DDOS attack
- Maskar, Virus
- Många paket per sekund
(attackerar router/switch/server CPU)
- Många bits per sekund
(attackerar bandbredden)

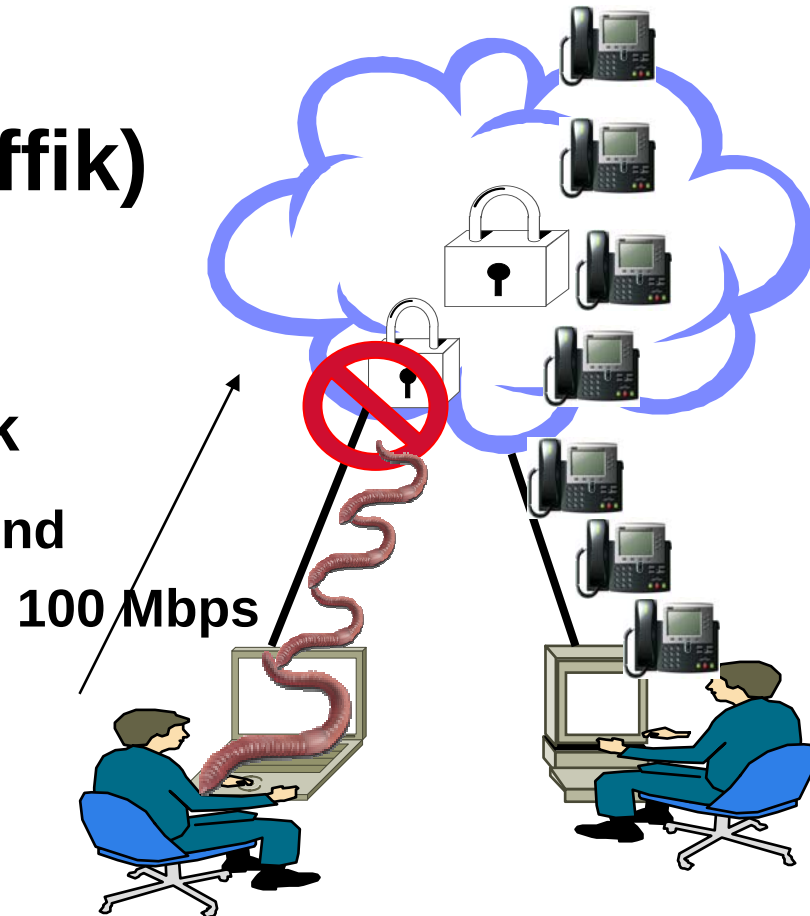


Skydd mot överbelastning

Cisco.com

QoS är en säkerhetsfunktion !

- Klassificera (märk all trafik)
- Vid överbelastning :
 - affärskritisk trafik
 - prioritera stryp misstänkt trafik
 - t.e.x fler syn-packet än 10 per sekund



Det Säkra Nätet : Cisco Network Admission Control (NAC)

Cisco.com

Uppfyller PCn säkerhetspolicyn :

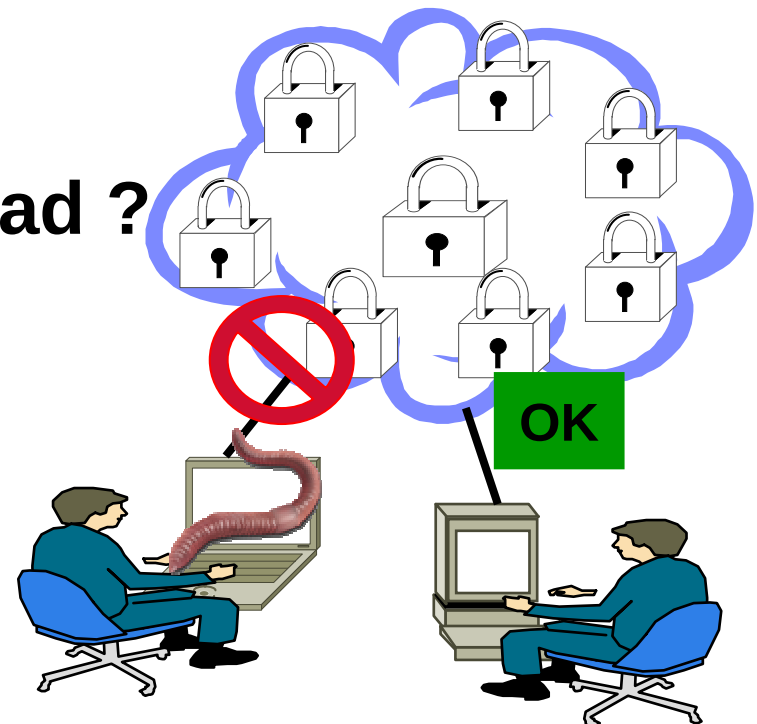
Rätt virusskydd ?

Rätt Microsoft Hotfix ?

Rätt browser ??

Personlig brandvägg installerad ?

oavsett anslutning
trådlöst, kabel eller via VPN....



Redo för ip telefoni ?

- **Organisation med andra verksamhetskritiska applikationer**
- **Organisation med kontroll över säkerheten (egen eller inhyrd kompetens)**

säkerhetspolicy

säkerhetsprocesser (t.e.x patchning av servrar, antivirus)

kontrollerad internetaccess, brandvägg, IPS

säkerhetsfunktioner i nätverket (t.e.x QoS)

monitorering...

Redo för ip telefoni ?

Cisco.com

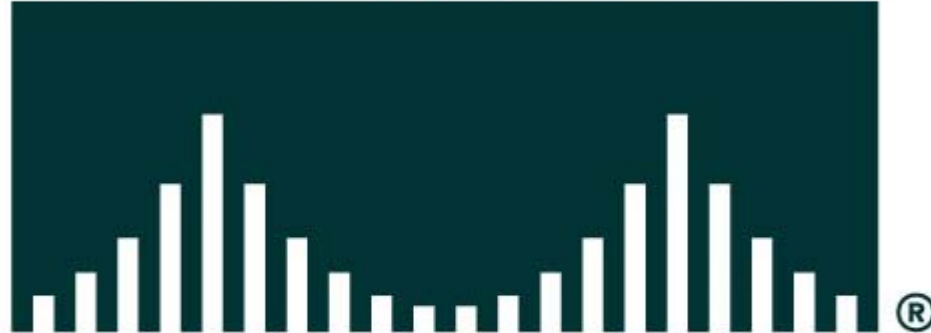
- **Organisation utan andra verksamhetskritiska applikationer**
- **Organisation utan kontroll över säkerheten**
 - saknar säkerhetspolicy**
 - saknar säkerhetsprocesser**
 - har brandvägg mot internet, men maskar orsakar ofta driftstopp**
 - nätverk utan säkerhet och qos funktioner**

- **IP telefoni – en applikation på ip nätet**
- **Kan säkras upp som andra verksamhetskritiska applikationer**
- **På samma sätt som andra verksamhetskritiska applikationer**
- **Ingen ny teknik egentligen : återanvänd samma processer, produkter, kompetens -> kostnadseffektivitet**

Läs Mer :

- <http://www.cisco.com/go/safe>
- http://www.cisco.com/en/US/netsol/ns340/ns394/ns165/networking_solutions_white_paper0900aecd80240249.shtml

CISCO SYSTEMS



EMPOWERING THE
INTERNET GENERATION