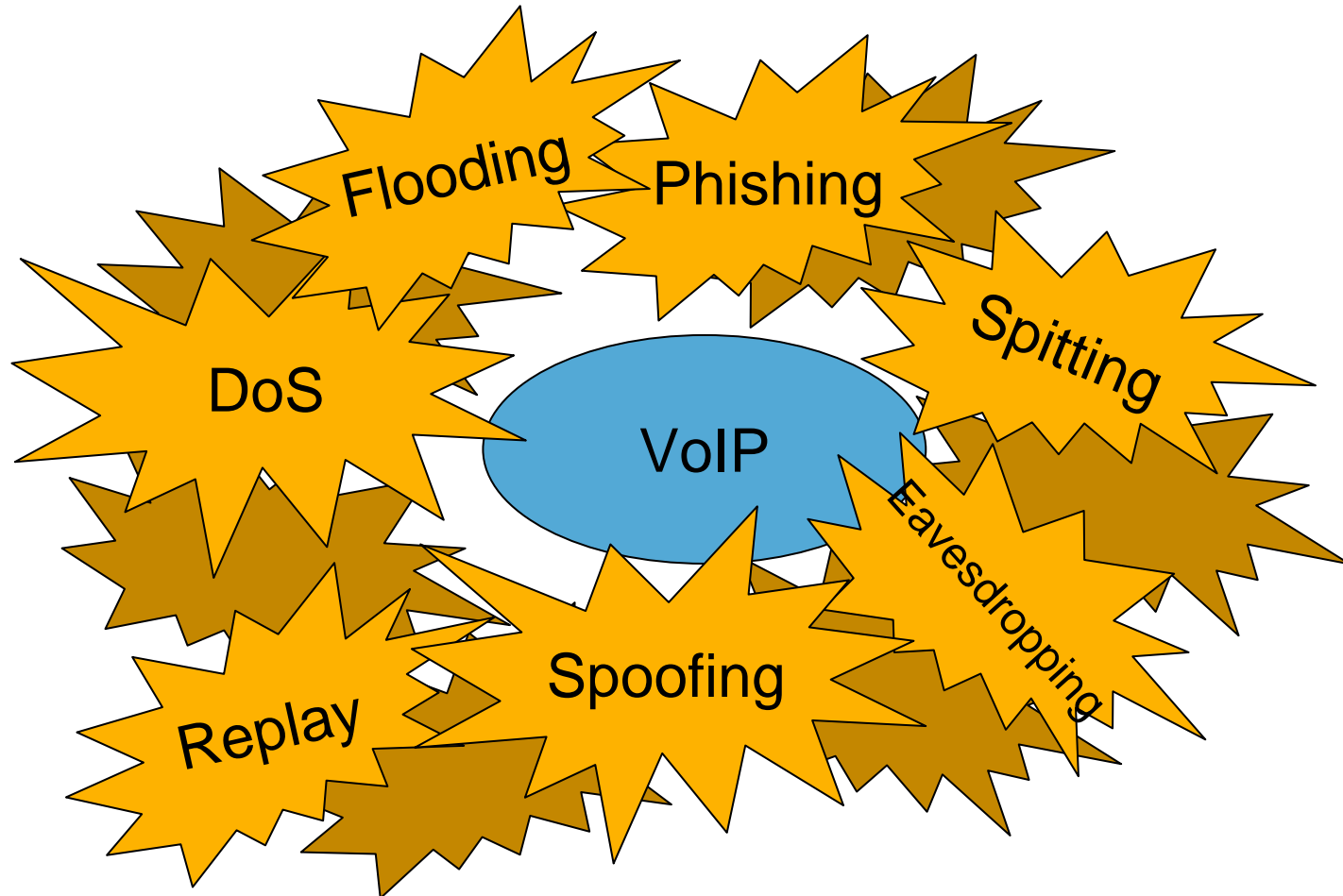


# Security und VoIP



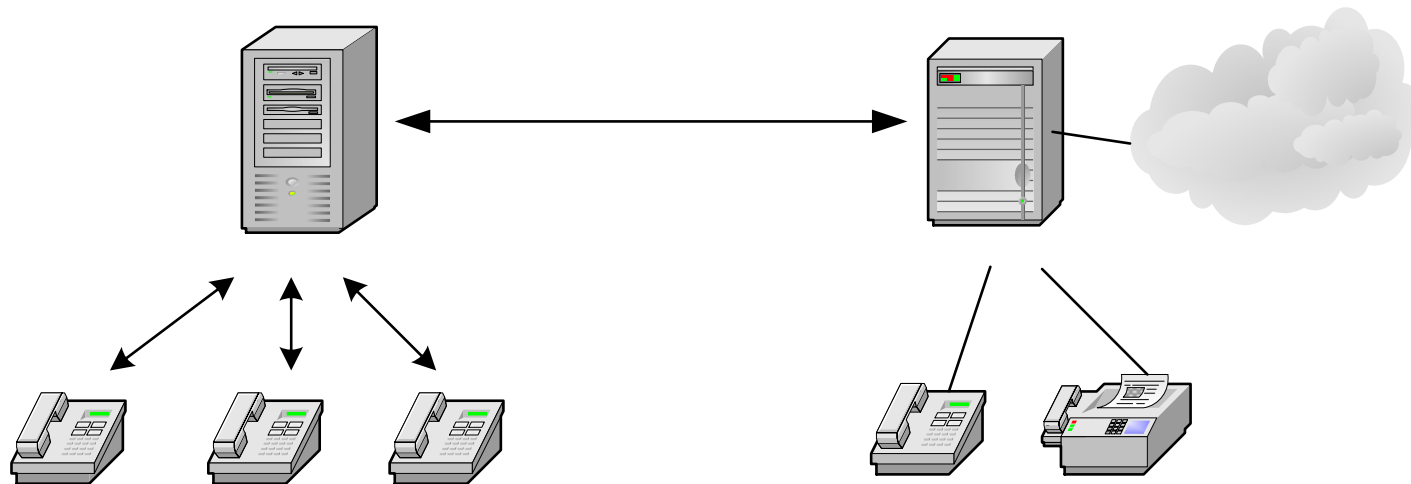
# VoIP und die Bedrohungen



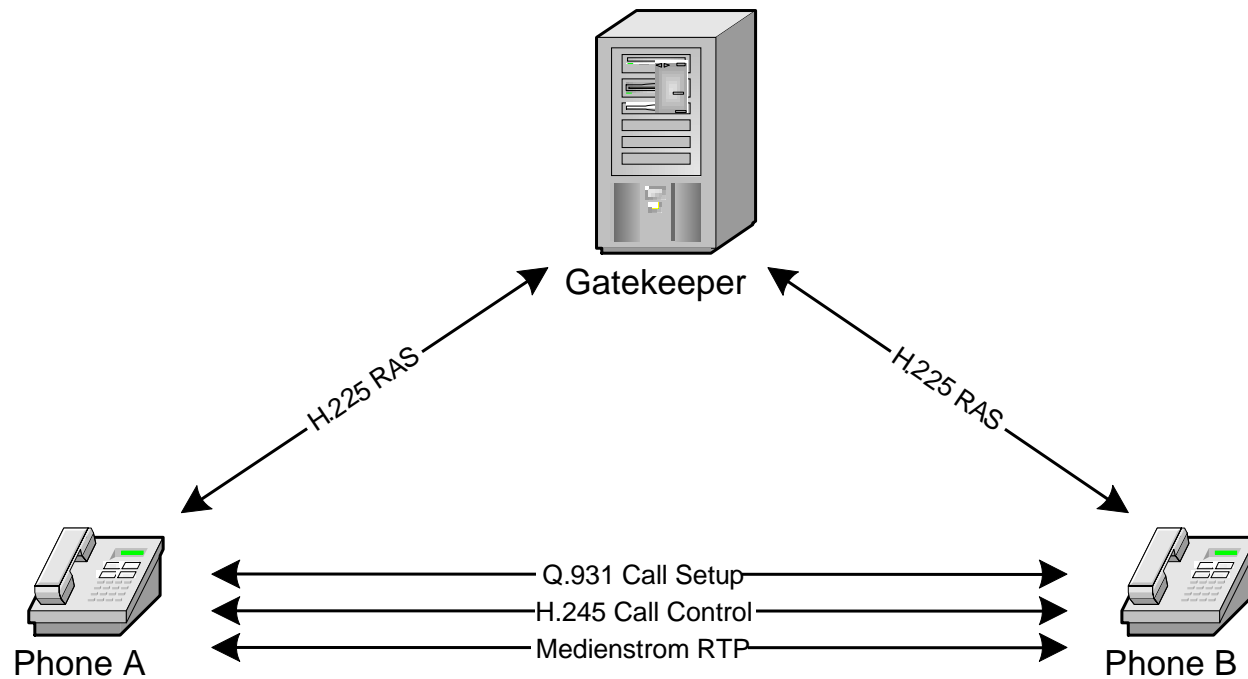
# VoIP-Technik

## Signalisierungsprotokolle

# H.323 Systemarchitektur



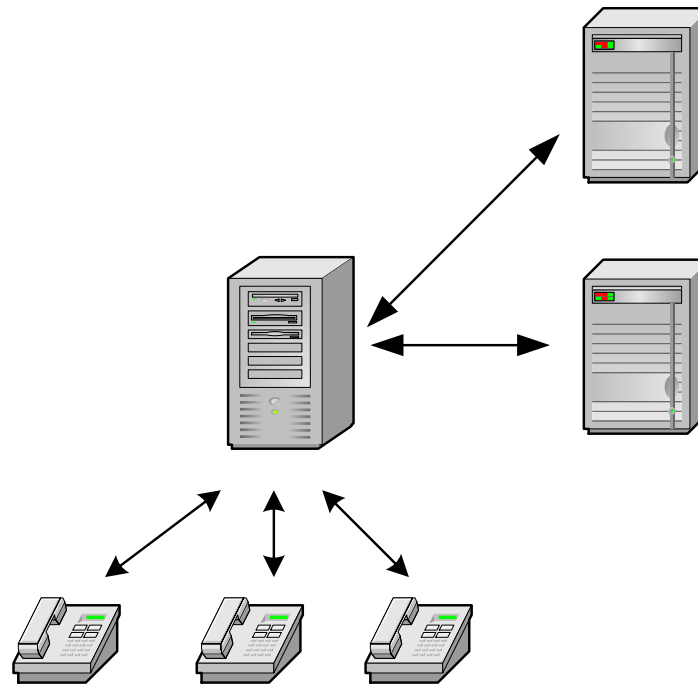
# H.323 Rufaufbau



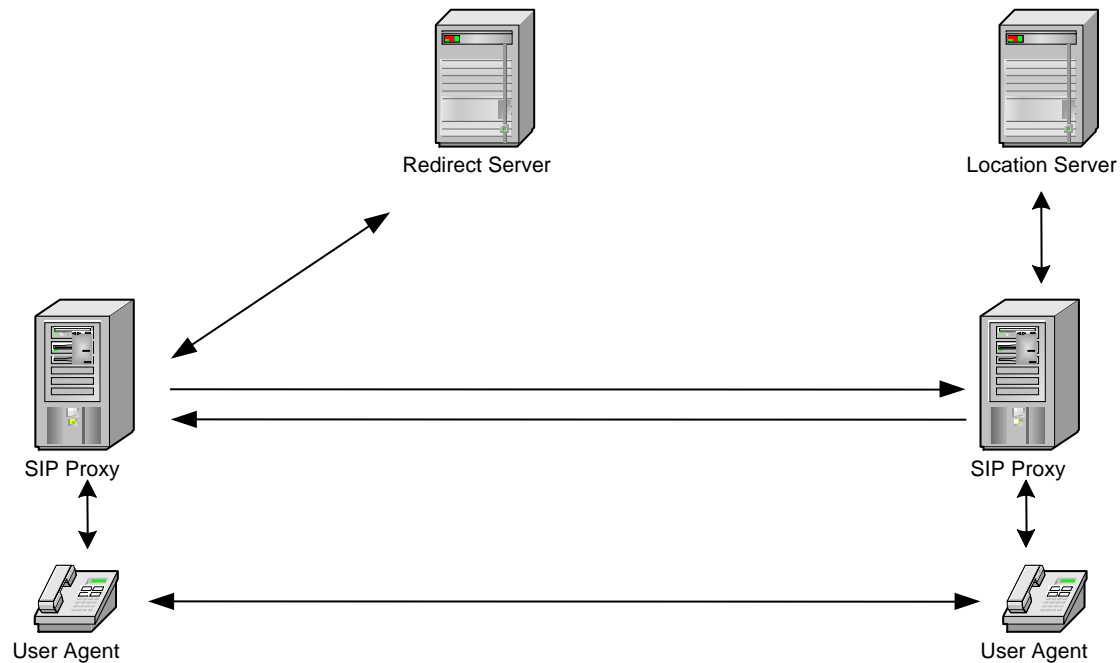
## H.323 Eigenschaften

- > Komplettes System für Multimedia (Audio und Video)
- > Angelehnt an ISDN, QSIG
- > Beschreibt Signalisierung und Medienübertragung
- > Integration in PSTN gegeben (z.B. Q.931)
- > Komplexe Struktur, viele Unterstandards

# SIP Systemarchitektur



# SIP Rufaufbau



# SIP Eigenschaften

- > Textbasierendes Signalisierungsprotokoll
- > Einfacher Aufbau, vergleichbar mit http
- > Adressierung ähnlich eMail-Adressen
- > Medienübertragung nicht definiert, beliebige Daten übertragbar
  - Telefonie, Instant Messaging, Gaming, ...
  - Meist RTP
- > Keine Interoperabilität mit PSTN
- > Durch geringe Komplexität gut skalierbar

# VoIP-Technik

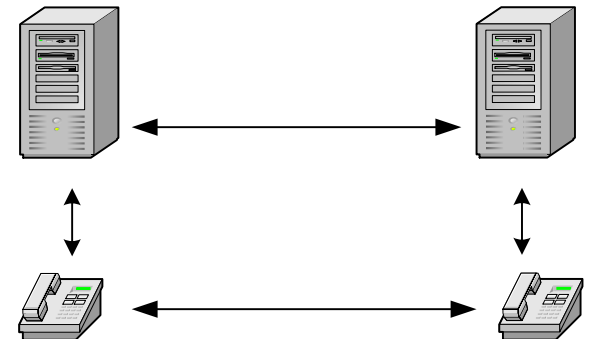
## Medienübertragungsprotokolle

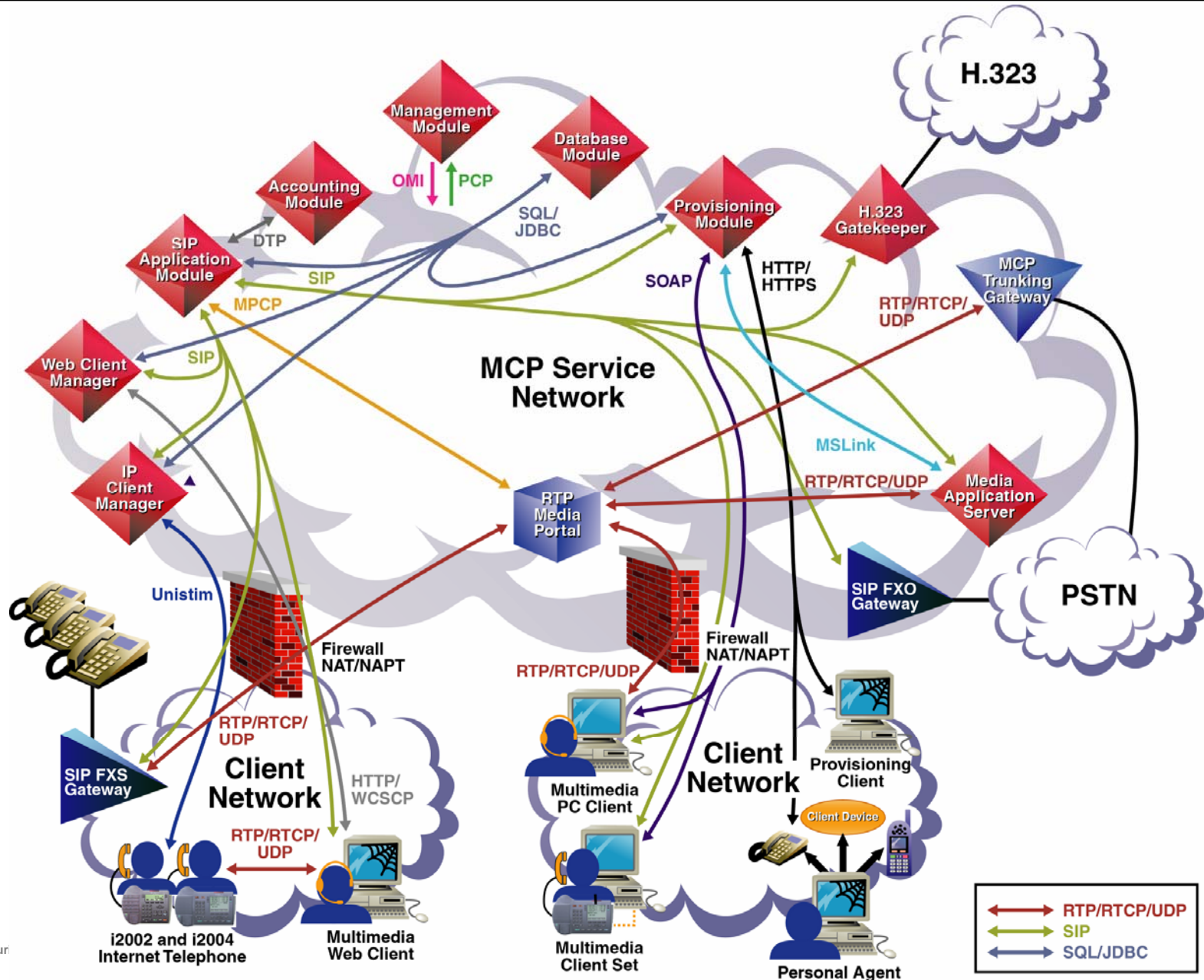
# RTP – Real-Time Transport Protocol

- > Bestandteil der H.323 Spezifikation
- > Sprach- und Videoübertragung
- > End-to-End Protokoll
- > RTP-Header
  - Codec (z.B. G.711, G.729)
  - Sequenznummer
  - Zeitstempel
  - Sync-Informationen
  - Verschlüsselungsalgorithmus (SRTP)
- > UDP-Transport
  - Timing wichtiger als Paketverlust
  - Codec korrigiert verlorene Sequenzen

# VoIP-Technik

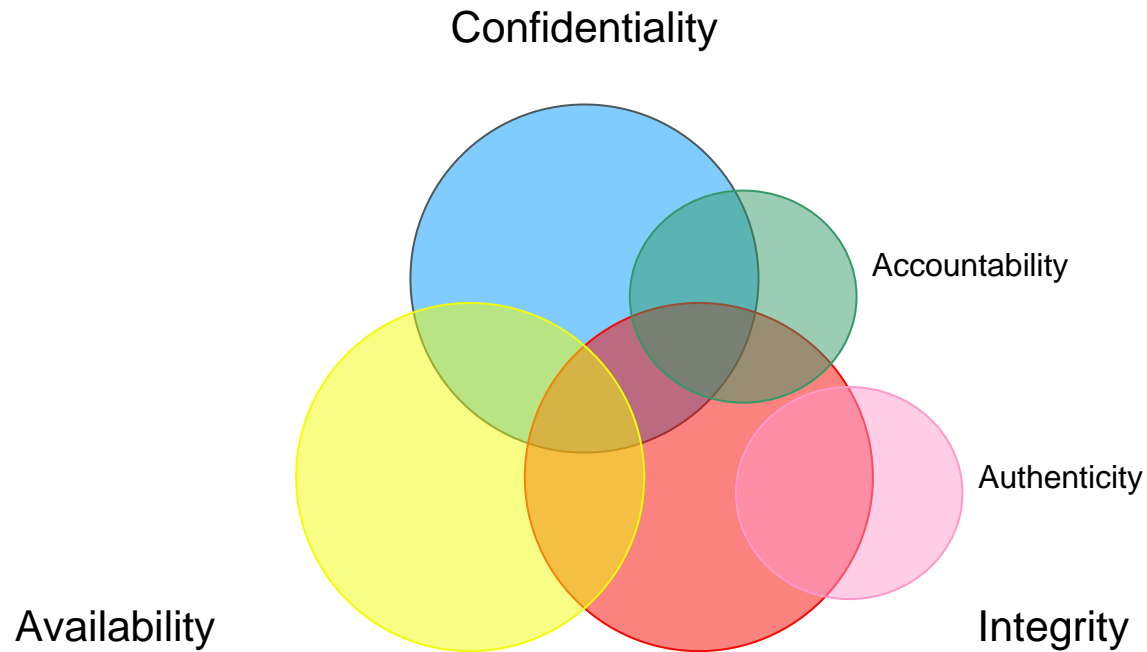
- > Gemeinsamkeiten der Protokolle
  - Rufnummern- bzw. Routingdatenbanken
  - Signalisierung Endgerät-Server bzw. Server-Server
  - Medienübertragung Endgerät-Endgerät
  - UDP-Kommunikation
  
- > Unterschiede zur klassischen Telefonie
  - Paket- statt sitzungsvermittelt
  - Transportmedium nicht für QoS errichtet
  - Gleiche Transportwege wie Datenströme
    - Auch jene von Fremdparteien (Internet)
  
- > Komplexe Struktur



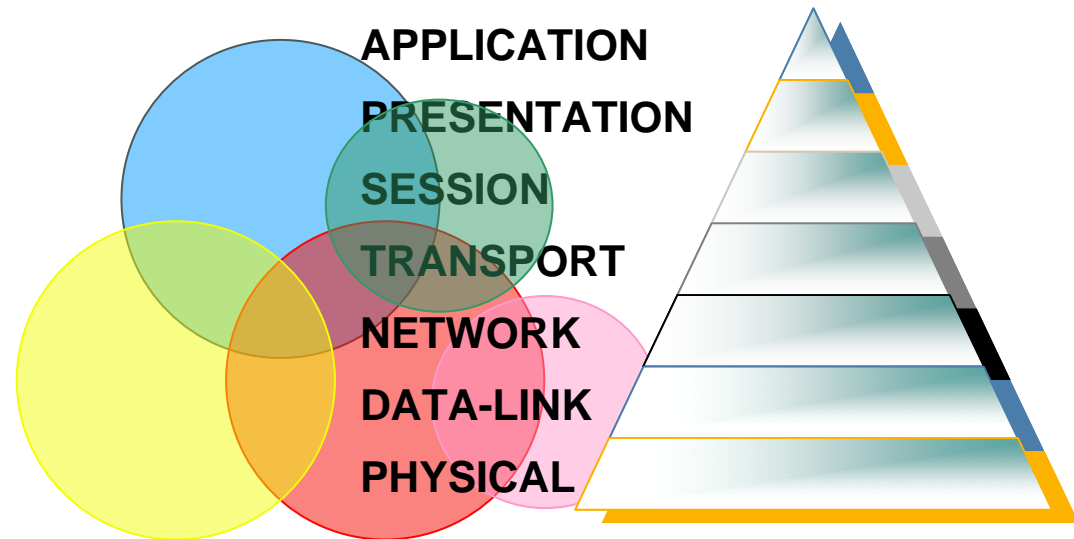


# VoIP Bedrohungen

# Security Evaluierung (C-I-A Triade)



# Security Evaluierung (C-I-A Triade)

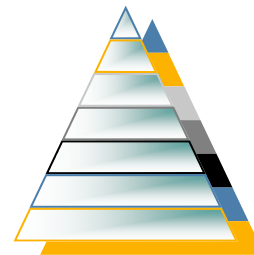
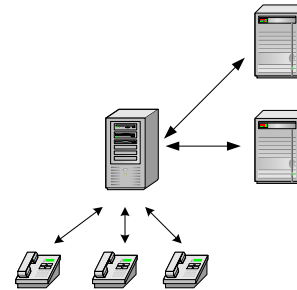
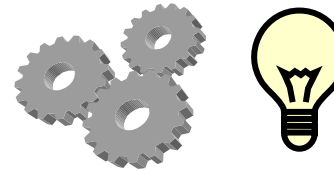


**Bedrohungen  
C-I-A**

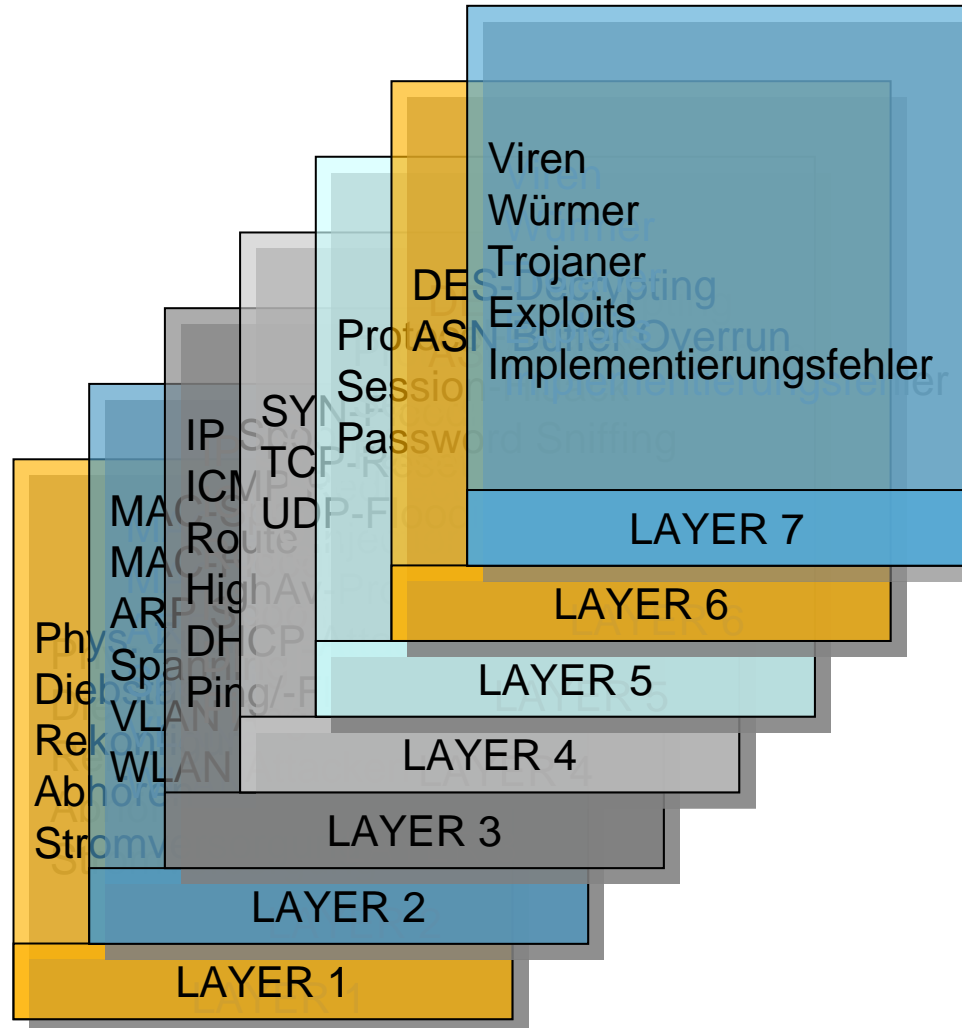
**Ebenen  
OSI-Layer**

# Klassifizierung eines Angriffes

- > Wer greift an?
  - Intern oder extern
  - Know-How, Ausstattung
  
- > Was wird angegriffen?
  - Endgerät
  - Server
  - Infrastruktur
  
- > Wo wird angegriffen?
  - Physisch
  - Netzwerk
  - Anwendung
  - Betriebssystem
  
- > Wie hoch ist die Bedrohung



# Bedrohungen - Netzwerk



# Bedrohungen der Infrastruktur – Layer 1

- > Phys. Zugriff
  - DoS
  - Diebstahl
  - Rekonfiguration
- > Abhören
  - Verkabelungssystem
  - Büros
- > Stromversorgung
  - Systeme
  - Endgeräte

# Bedrohungen der Infrastruktur – Layer 2

- > MAC-Spoofing
- > MAC-Flooding
- > ARP Spoofing
- > Spanning Tree Attacken
- > VLAN Angriffe
- > WLAN
  - MAC-Filtering
  - SSID
  - WEP

# Bedrohungen der Infrastruktur – Layer 3

- > IP Spoofing
- > ICMP Redirect
- > Route Injection
- > HA-Protokolle (HSRP, VRRP)
- > DHCP Attacken
- > Ping/SYN-Flooding

# Bedrohungen der Infrastruktur – Layer 4

## > RTP

- Decodierung des Datenstroms
- Manipulation der Übertragung

## > H.323

- VoIP-Address Spoofing
- Man-in-the-Middle Attacke
- Passwort-Authentifizierung in Klartext
- IP-Spoofing im Transport

## > SIP

- Header-Manipulation
- Alle Angriffe wie bei H.323, nur einfacher (ASCII-formatiert)

# Bedrohungen der Infrastruktur – QoS

- > QoS-Parameter
  - Bandwidth
  - Packet Loss
  - Delay
  - Jitter
  
- > QoS-Bedrohungen
  - Netzüberlasten
  - Konfigurationsfehler
  - DoS, DDoS
  - QoS-Attacken

# Bedrohungen der Infrastruktur – Systeme

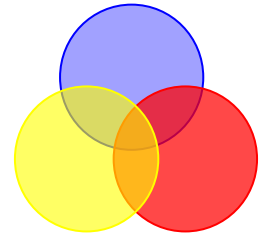
- > VoIP-Systeme
  - Netzwerkangriffe
  - OS-basierende Angriffe
  - Angriffe auf Basisdienste
  
- > VoIP-Endgeräte
  - Netzwerkangriffe
  - OS-basierende Angriffe
  - Angriffe auf Basisdienste
  
- > Gateways
  - Fernwartungszugänge
  - Hijacking

# Bedrohungen auf Anwendungsebene

- > Viren, Würmer, Trojaner
- > Exploits
- > Implementierungsfehler

# Sicherheitsmaßnahmen

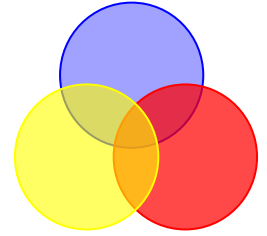
# Sicherheitsmaßnahmen – Layer 1



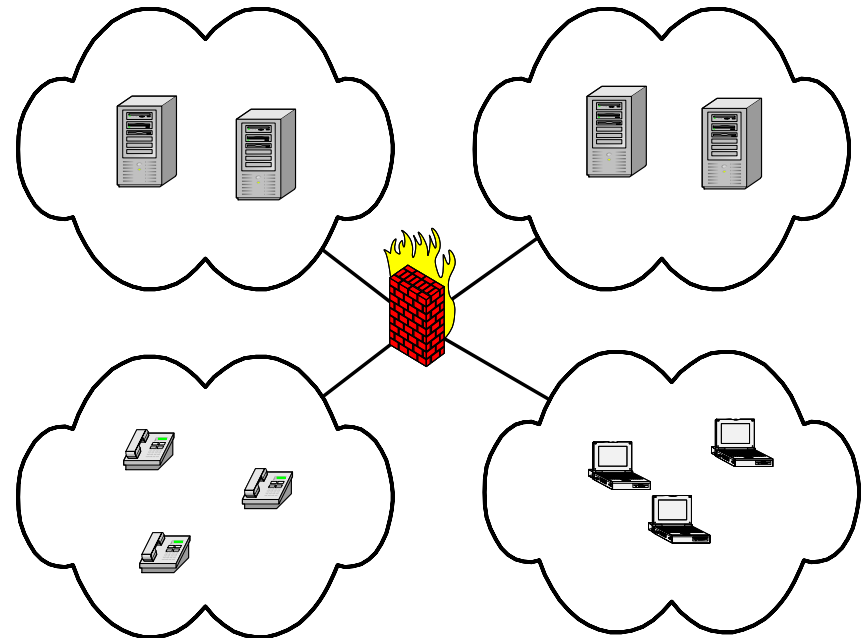
- > Serverräume, Netzwerkverteiler
  - Zutrittsschutz und Überwachung
  - Environment (Feuer, Wasser, Klima)
- > Verkabelungssysteme
  - Redundante Struktur
  - Zutritt zu Steigschächten
  - Abhörsichere Verkabelung
- > Stromversorgung
  - Redundante Versorgung kritischer Systeme
  - Unterbrechungsfreie Stromversorgung
  - Power over Ethernet



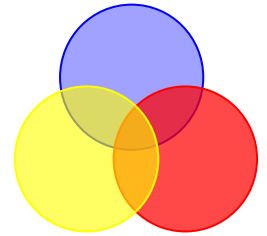
# Sicherheitsmaßnahmen – LAN



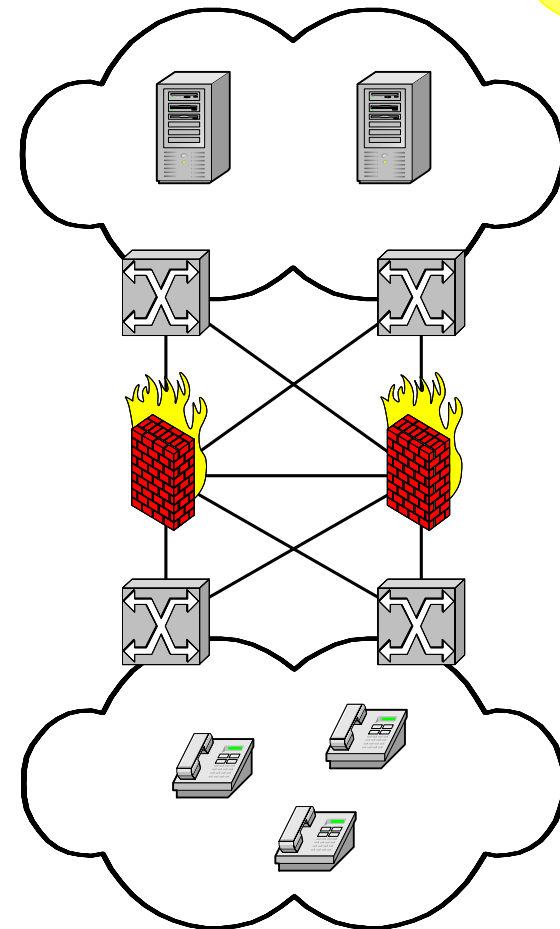
- > VLAN-Struktur
  - Getrennte Daten- und Voice-VLANs
  - Firewalling zwischen VLANs
  - CoS, QoS per VLAN
  
- > Authentifizierung 802.1x
  - In Kombination mit VLAN-Struktur
  - EAP-TLS/EAP-MD5/PEAP
  - Endpoint-Security



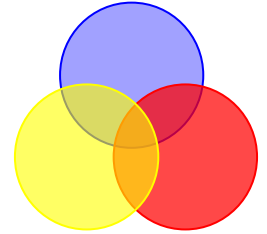
# Sicherheitsmaßnahmen – LAN



- > Redundanz
  - STP, RSTP
  - VRRP
  - Firewall-Clustering
  - Server-Clustering

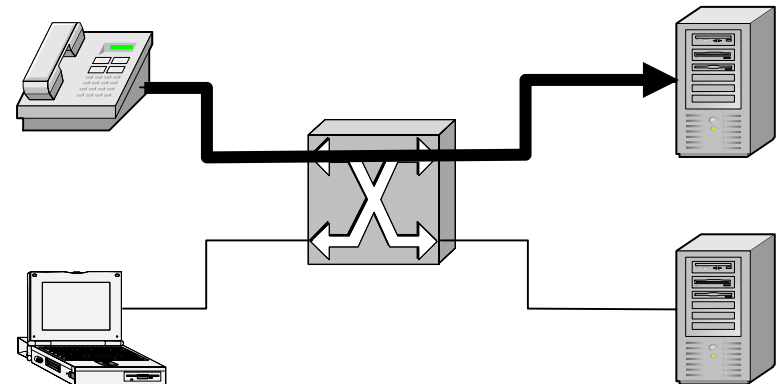


# Sicherheitsmaßnahmen – LAN

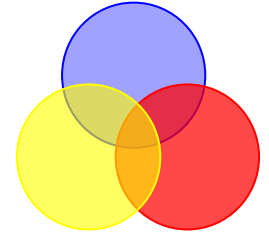


## > Quality of Service

- CoS 802.1p
- DiffServ
- RSVP
- Bandbreitenmanagement



# Sicherheitsmaßnahmen - LAN



## > Firewalling

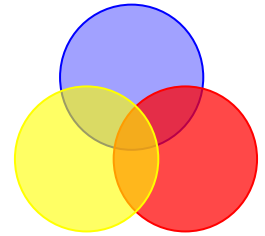
- Firewall muss VoIP verstehen
  - UDP-Kommunikation
  - Dyn. Ports für Medienübertragung
- Verbindungsmatrix
  - End-to-End
  - End-to System
  - System-to-System
- QoS

⊕ VoIP-Segment1	☎ Gateway1	*	UDP sip	⊕ accept
⊕ VoIP-Segment1	⊕ VoIP-Segment2	*	?? sip_dynamic_port UDP sip_any	⊕ accept
☎ Gateway1	☎ Gateway2	*	TCP H323	⊕ accept
⊕ VoIP-Segment2	☎ Gateway2	*	UDP H323_ras	⊕ accept

## > NIDS

- Protocol Inspection
- UDP Flooding
- Positionierung der Probes!

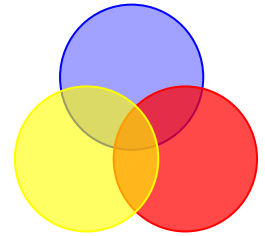
# Sicherheitsmaßnahmen – WAN/Internet



## > Firewalling

- NAT-Problematik bei VoIP
  - RTP verwendet dynamische Ports
  - Portverhandlung erfolgt in der Session Description
  - IP und Port werden im Datenfeld übertragen
  
- Klassische Firewalls übersetzen nur IP-Header, jedoch nicht das Datenfeld

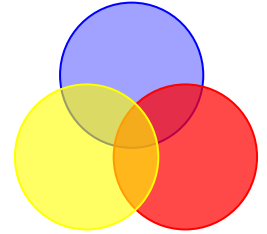
# Sicherheitsmaßnahmen – WAN/Internet



## > Firewalling

- Intelligentes VoIP-NAT
  - Firewall erkennt und übersetzt IP im Datenfeld
  - Statisches und dynamisches NAT
- MidCom
  - Middlebox (NAT-Device) wird vom Gatekeeper gesteuert
- SBC
  - Session Border Controller wickelt Signalisierung und Medientransport ab

# Sicherheitsmaßnahmen – WAN/Internet

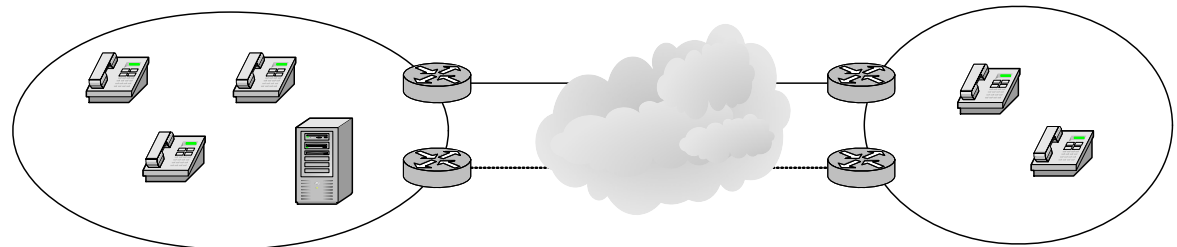


## > QoS

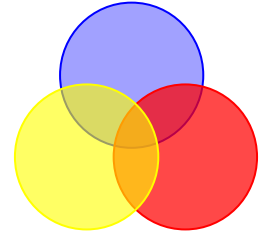
- Priorisierung am Edge-Router
- QoS-fähiges WAN (z.B. MPLS)
- Dienstgüte im WAN
  - Packet Loss, Delay, Jitter
- Überlastbehandlung

## > Redundanz

- Multi-Peering
- Backup-Routen

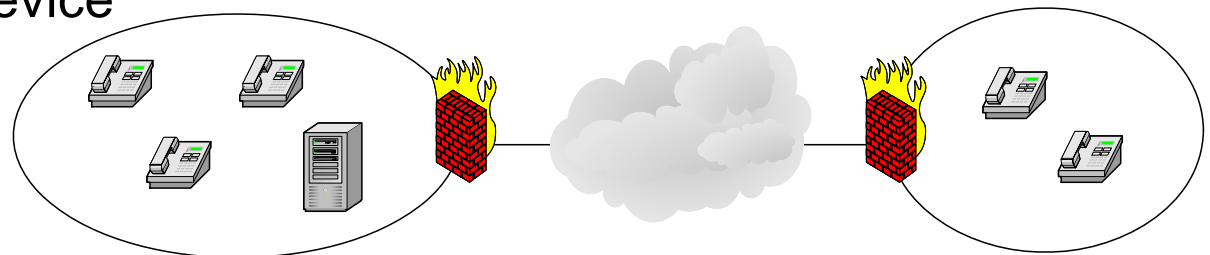


# Sicherheitsmaßnahmen – WAN/Internet

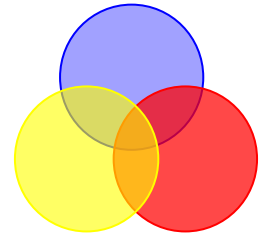


## > VPN

- Site-to-Site VPN
  - Encryption/Authentication
  - Ausfallsicherheit
- Client-VPN
  - Softphone
  
- QoS im VPN
  - VoIP-Header wird mitverschlüsselt
  - QoS vor VPN
  - QoS im VPN-Device
  - IPv6



# Sicherheitsmaßnahmen – Systeme

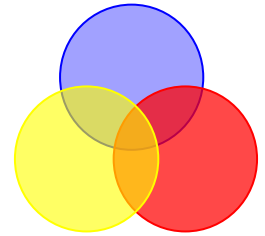


## > Betriebssystem

- Out-of-Band Management
  - Authentifizierung
- Admin-Zugänge nur verschlüsselt
  - ssh, https
  - Management-VLAN
- OS-Hardening
  - Minimalsystem
  - Security-Patches
- Backup
  - Clustering
  - Datensicherung
  - Redundanz der Systeme/Applikationen

## > HIDS

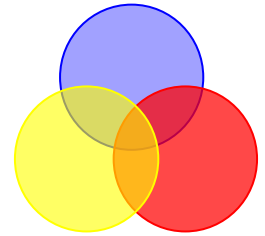
# Sicherheitsmaßnahmen – Systeme



- > Secure Proxies
  - Gateway zwischen sicheren und unsicheren Systemen
  
- > Signierte Firmware Images
  - Korrekte Type
  - Schutz vor modifizierten Images
  - Signierte Konfigurationsdateien

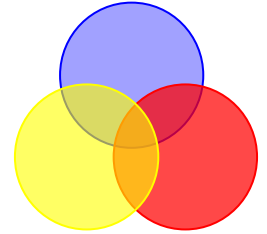


# Sicherheitsmaßnahmen – Protokolle



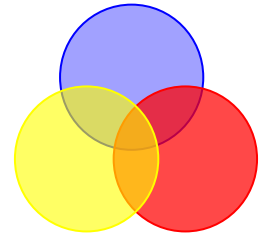
- > Sichere Signalisierung in H.323 (H.235v3)
  - Einsatz kryptografischer Verfahren
    - IPSec oder TLS
  - Media Antispam
    - Message Authentication mit SHA1-96
  - Hop-by-Hop Authentication
    - Benutzer, Signalisierung
  - Direkte Signalisierung
    - Key-Exchange zwischen Endgeräten
    - Gatekeeper wird zum Key Distribution Center
  - SRTP

# Sicherheitsmaßnahmen – Protokolle



- > Sichere Signalisierung in SIP (SIP 2.0)
  - HTTP Digest Authentication
    - Hop-to-Hop
    - Auf allen SIP-Komponenten implementiert
    - Keine Integrität/Authentizität der Gesamtnachricht
      - Ergänzung z.B. mit TLS
  - S/MIME
    - SIP-Nachricht ähnelt E-Mail
    - SDP-Body signiert und ggf. verschlüsselt
    - Sicherer Key-Exchange z.B. für SRTP
  - SIP über TLS
    - Hop-to-Hop
    - UDP->TCP
  - SIP über IPSec

# Sicherheitsmaßnahmen – Protokolle

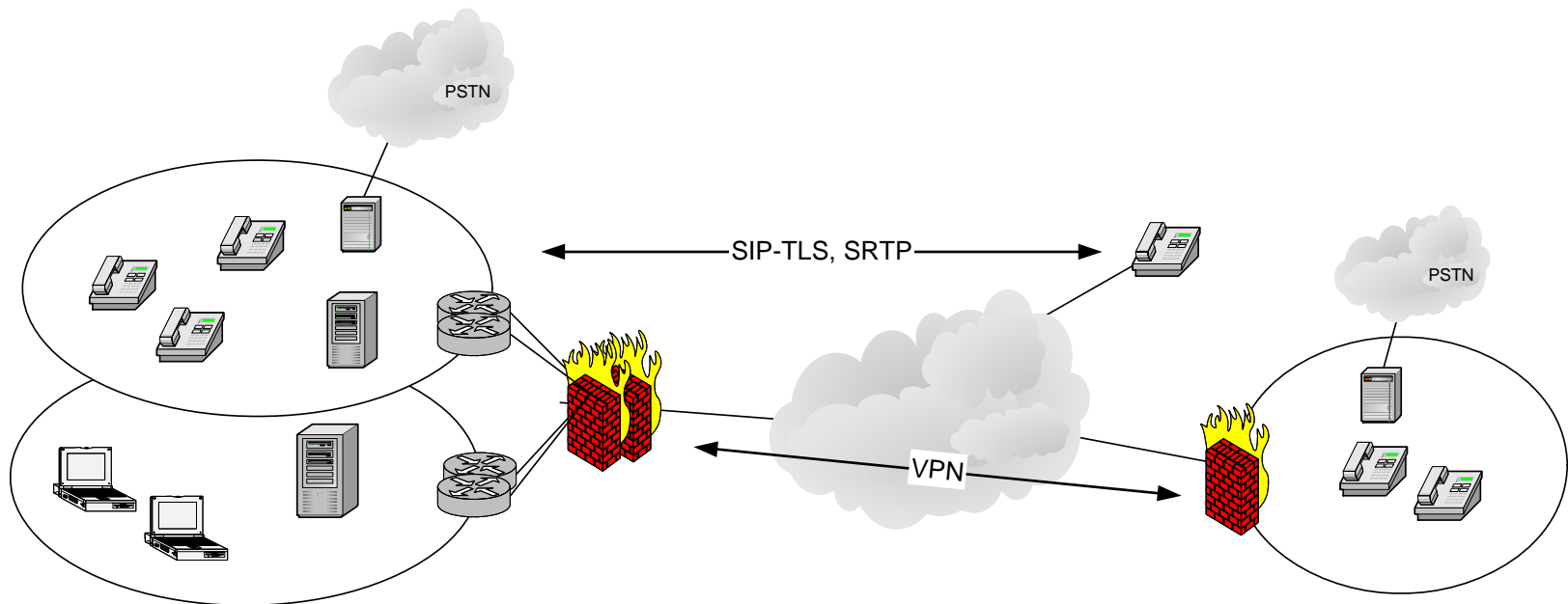


- > Zertifikate im Phone
  - Vendor-Hardcoded
  - Soft-Zertifikate
  
- > Sichere Medienübertragung SRTP
  - Verschlüsselung, Authentifizierung
    - AES, SHA-1
  - Replay-Schutz
  - Key-Management MIKEY
  
- > IPSec
  - Für VoIP nur bedingt geeignet, da
    - QoS-Problem
    - Timing des Key-Exchanges
    - ESP-Overhead
    - CPU-bedingte Latenz im Endgerät

# Welche Vorgehensweise?

# Security-Konzept

- > Kombination von Security-Maßnahmen
  - Geeignete Techniken einsetzen
  - Synergien nutzen



# VoIP-Security am Markt

- > VoIP-Systeme
  - Vermehrt Einsatz von SRTP, SIP-TLS
  - Proprietäre Lösungsansätze (Secure SCCP, Secure UNISlim, ...)
  
- > LAN-Komponenten
  - QoS Standards
  - 802.1x, Multi-Authentication, Endpoint Security
  
- > VoIP-Firewalls
  - Kompatibel zu VoIP-Protokollen
  - Integriertes QoS

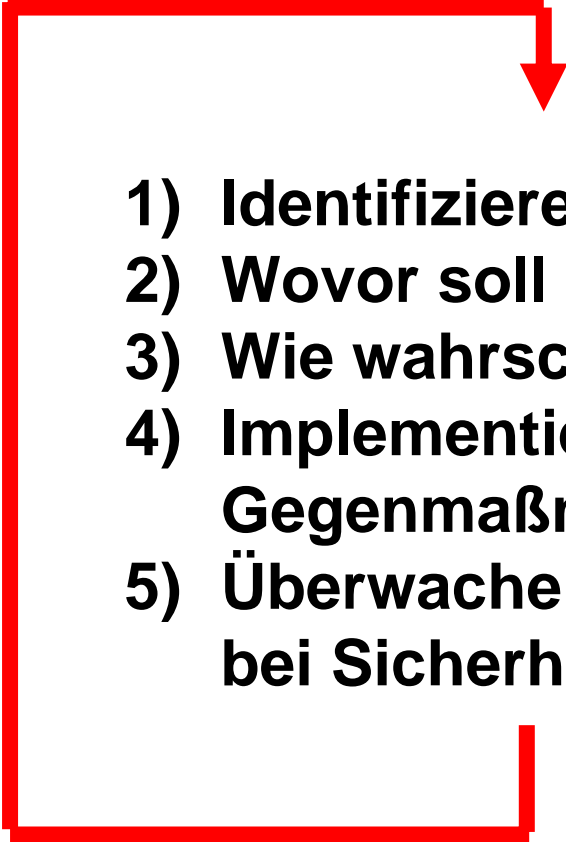
# Ihre Entscheidung

- > Security ist ein Entscheidungskriterium
  - Funktionalität und Security als Gesamtkonzept
  - VoIP wird mehr und mehr Plug-and-Play, VoIP-Security nicht
  - Nehmen Sie den Lieferanten in die Pflicht
  
- > Nutzen Sie Ihre bestehenden IT-Systeme
  - Viele Sicherheitsfeatures sind bereits integriert (Switches)
    - Sie müssen oft nur aktiviert werden
  
- > Erstellen Sie ein Sicherheitskonzept
  - Überlegen Sie die für Ihr System geeigneten Maßnahmen
  - Beachten Sie C-I-A
  - Beachten Sie die OSI-Layer

# Zukunft

- > Komplexität
  - IP-Phones leisten immer mehr
    - Kalender, ToDo-Listen, Medienwiedergabe, Browser
  
- > Erweiterbarkeit
  - Mobile Code am Phone
    - Java
    - API's
  
- > Connectivity
  - WLAN-Hotspots
  - Mobile SoftPhone

# RFC 2196 Herangehensweise

- 
- 1) Identifiziere, was du beschützen willst.**
  - 2) Wovor soll es geschützt werden?**
  - 3) Wie wahrscheinlich ist die Bedrohung?**
  - 4) Implementiere kostengünstige Gegenmaßnahmen.**
  - 5) Überwache den Prozess und nimm Korrekturen bei Sicherheitsverstößen vor.**

# Conclusio

- > VoIP-Security Standards und Techniken existieren
  - Umsetzung in den Systemen schreitet voran
  - Implementierung teilweise noch mangelhaft
  - Überarbeitung der Standards notwendig
  
- > IT-Infrastruktur kann Lücken schließen
  - Viele Techniken der IT-Security anwendbar
  - QoS als wesentliches Unterscheidungsmerkmal
  
- > Einsatz von VoIP dem Stand der (Security-)Technik anpassen

# Vielen Dank für Ihre Aufmerksamkeit

Enabling effective real time business