Policy Based Networking = cesta jak zajistit QoS

Petr Lasek

VUMS DataCom

22.3.2001

Konference vysokorychlostní sítě

www.datacom.cz

Allot Communications

www.allot.com

Rychlost = kvalita služeb?

Allot Communications

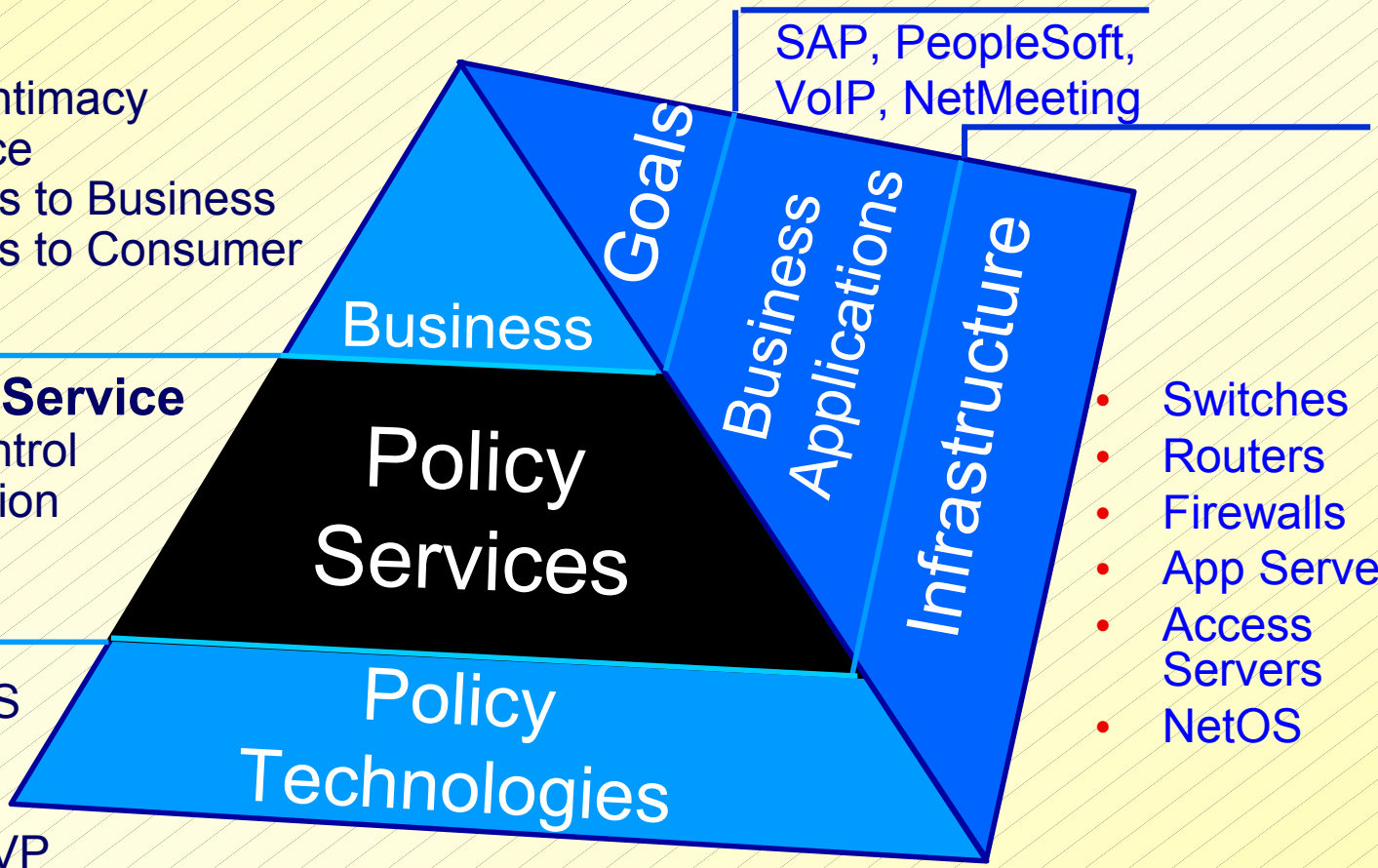
Parametry ovlivňující QoS

- Šířka pásma (bandwith)
- Zpoždění (delay)
- Rozptyl zpoždění (jitter)
- Ztrátovost (packet loss)
- Dostupnost (availability)

Allot Communications

Policy*)-based Networking

- Customer Intimacy
- E-Commerce
  - Business to Business
  - Business to Consumer



Quality of Service

- Access Control
- Authentication
- Reliability
- Priority

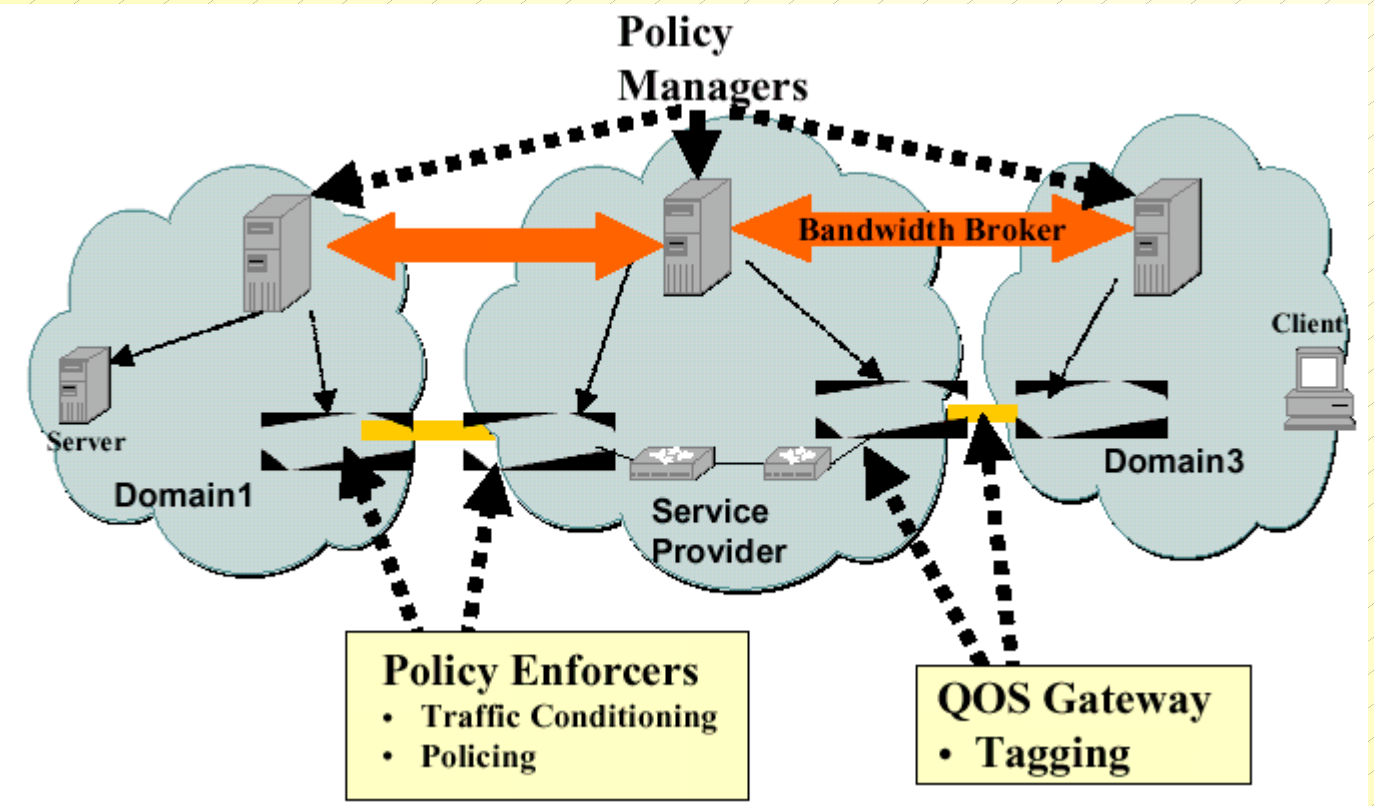
- DHCP, DNS
- RADIUS
- LDAP
- COPS, RSVP
- 802.1p, DiffServ

- Switches
- Routers
- Firewalls
- App Servers
- Access Servers
- NetOS

*) postup, taktika, plán, metoda, politika

Allot Communications

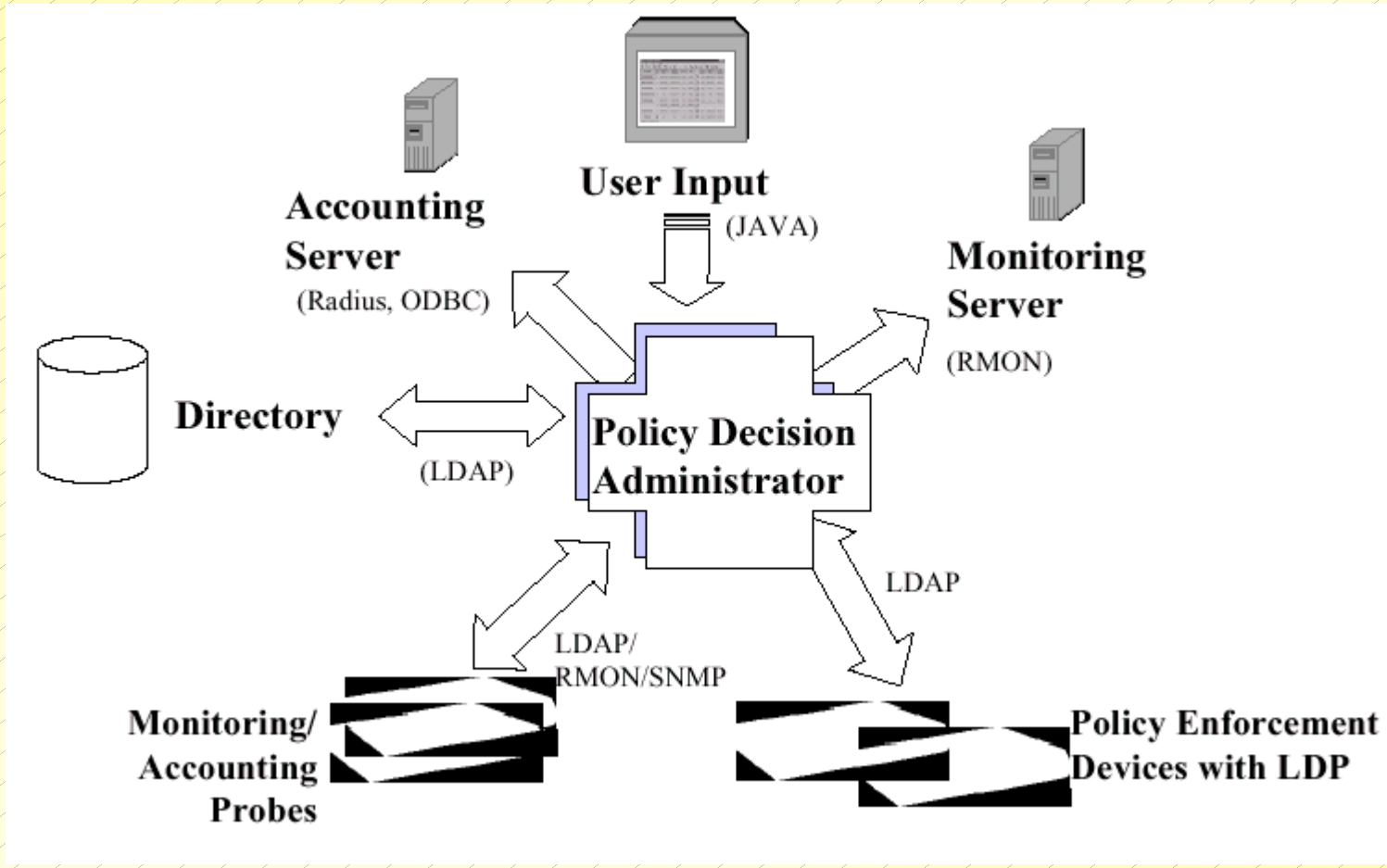
Architektura



- PDP (Policy Decision Point)
- PEP (Policy Enforcement Point)
- Adresářové služby (DEN – Directory Enabled Network))

Allot Communications

Policy Management



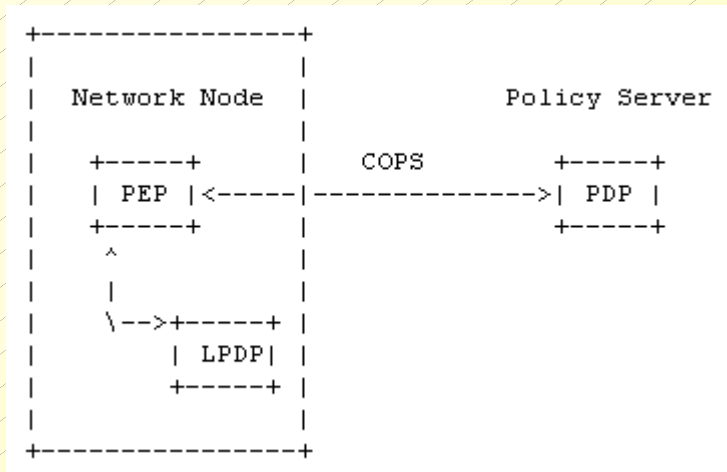
Data Abstaction Layer
Device Abstraction Layer

CIM (Common Information Modul)

- „Taxonomie“ sítě
- Objektový model
- DMTF (Distibuted Management Task Force)
  http://www.dmtf.org/spec/cims.html
- Současná verze 2.5
- Policy informace: IETF – RFC 3060
  http://www.ietf.org/rfc.html
- Namapování CIM do adresářových služeb (DEN = Directory Enabled Network)

COPS

- Common Open Policy Service
- RFC 2748
- TCP, klient/server
- Výměna informací mezi PEP a PDP
- Pokud prvek nepodporuje COPS – SNMP, LDAP, CLI



Allot Communications

Co nabízí Allot?

Organizational Information

- Applications
- Users
- Resources

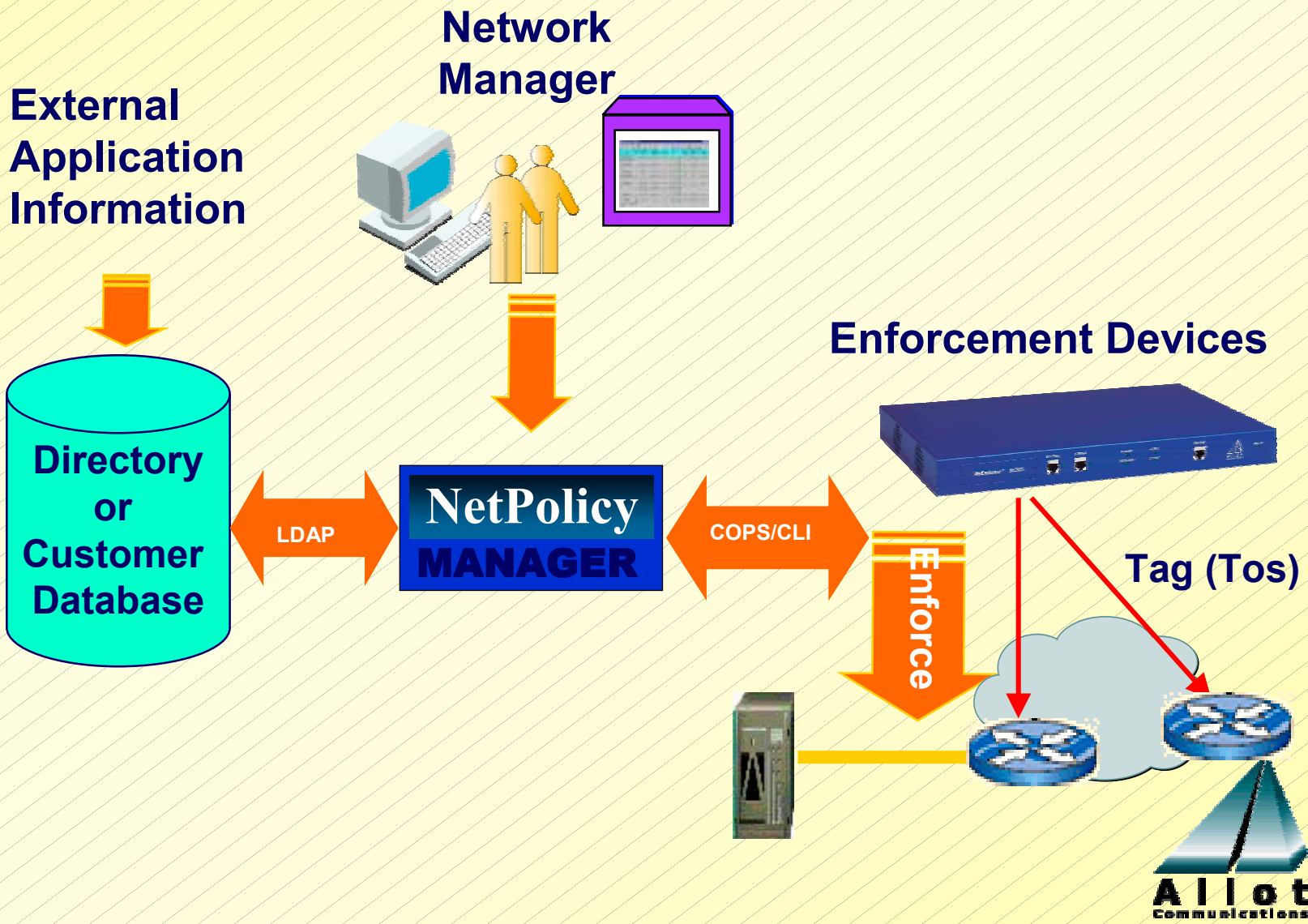
Policy-Based Control

Network Actions
Delivering QoS

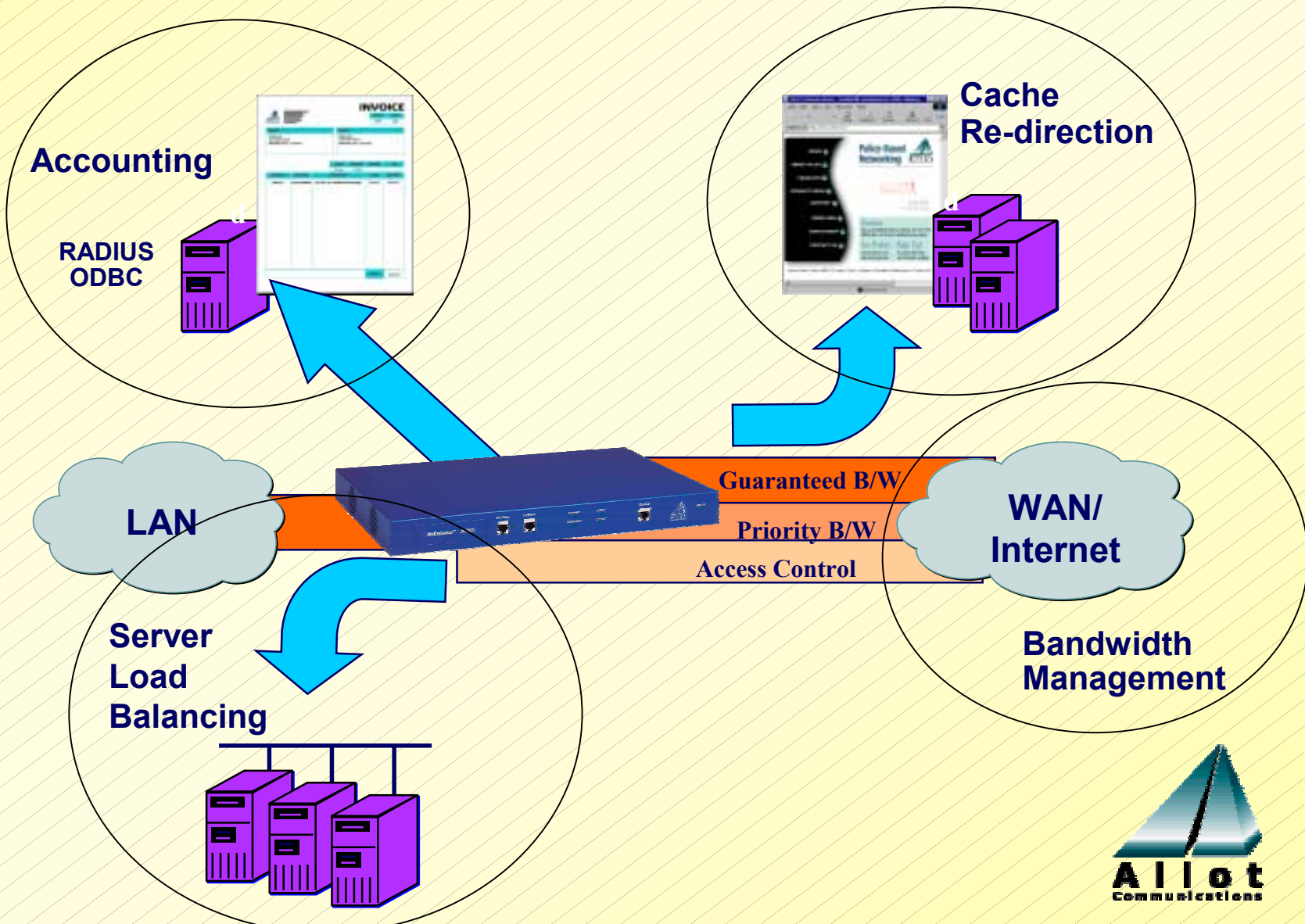
- Shape Bandwidth
- Load Balance Servers
- Virtual Leased Lines
- Cache Redirection
- Accounting
- Access Control

Allot Communications

"Policy“ Architektura



The Solutions Family



Allot Comprehensive Solution

NetPolicy MANAGER

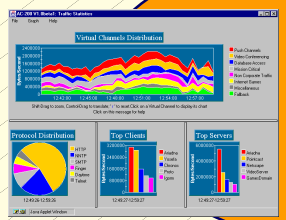
Prosazování QoS

- Formování provozu (Traffic Shaping)
- Přidělování priorit
- Podmínky pro mission-critical aplikace
- Garantování SLA
- QoS Tagging

Policy a SLA Management

- Překlad pravidel na odpovídající akci v síti
- Distribuce pravidel do PEP (NetEnforcer, CISCO, RADGuard)
- Management aplikací
- Management uživatelů (adresářové služby)

Monitoring a Accounting



- Monitorování pravidel
- Accounting and Billing
- Event Management
- Sledování služeb

Allot Communications

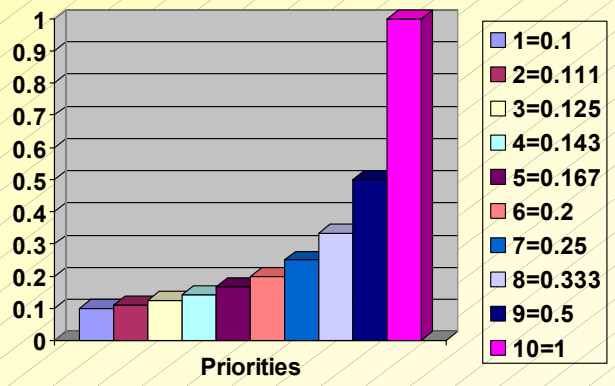
Quality of Service

- Přidělování priorit podle aplikací nebo uživatelů
- Maximální a minimální rychlost (CIR/MIR)
  - Omezování a garantování šířky pásma
  - Lze pro příchozí/odchozí směr nezávisle
- CBR - Constant Bit Rate (virtuální pevná linka)
  - Voice over IP, ...
- Maximální počet spojení na uživatele/aplikaci
- TOS (označování paketů)
- Povolení zakázaní uživatele/aplikace v síti

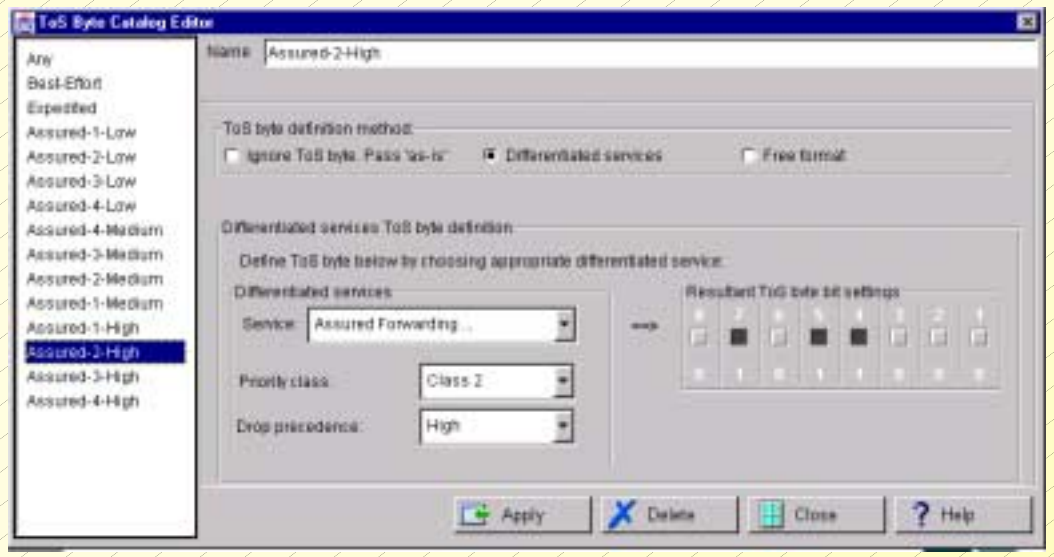
Allot Communications

Quality of Service

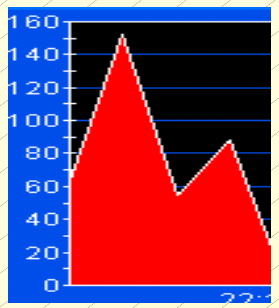
Priority (10)

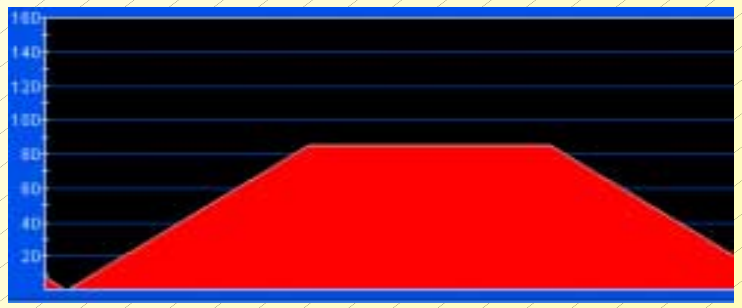


TOS



CIR/MIR

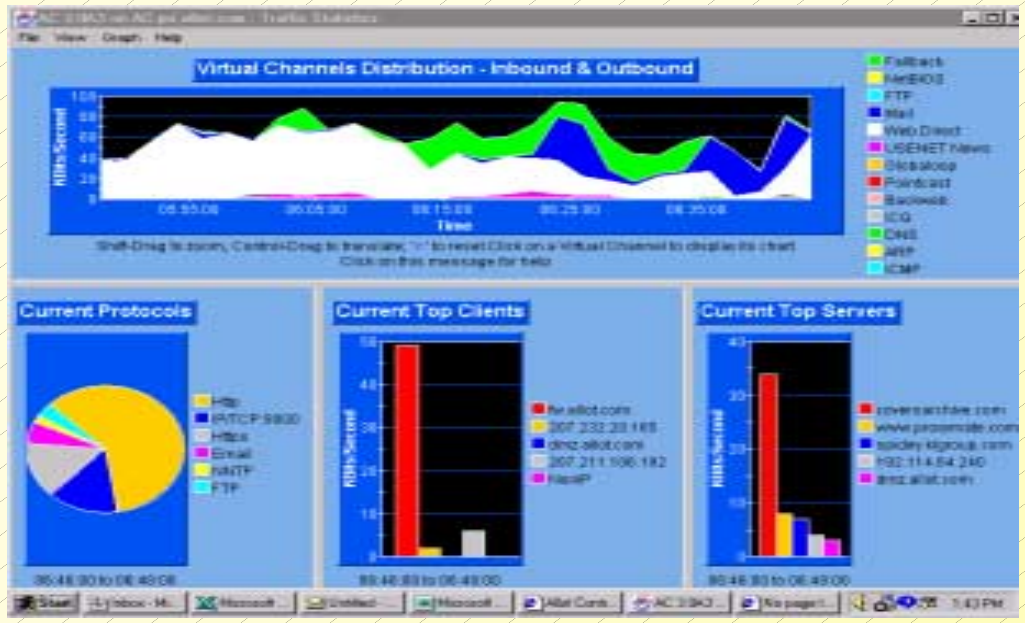




Allot Communications

Monitoring

- Statistiky v reálném čase
- Nejaktivnější uživatelé a aplikace
- Protokolová analýza
- "Přehled a pochopení" co se v síti děje



Allot Communications

Load-Balancing

- Vyvažování zátěže mezi servery
- Redundance a vysoká dostupnost
- Úspory za drahý HW
- Zvýšená bezpečnost (VIP – virtual IP)
- Snadná kombinace s QoS

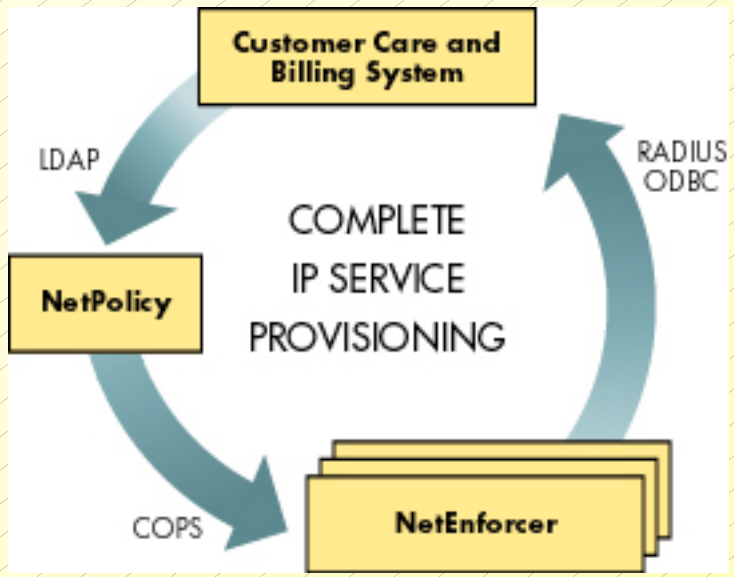
Allot Communications

Cache Redirection

- Úspora provozu ve WAN
- Není nutno konfigurovat klienty
- Možnost rozlišovat, který provoz bude přesměrován do cache
- Záložní cache nebo více cache
- Kombinace s QoS

Accounting

- Dlouhodobé reporty o provozu v síti
- Zpětná kontrola stavu sítě (obdoba RMON2 sondy)
- Podklady pro billing
- Automatické generování reportů
- Spolupráce s Radius, ODBC nebo lze exportovat v CSV formátu



Rodina produktů NetEnforcer

NetEnforcer AC101

Do 512 Kbps,
1000 současných spojení.
Volitelně všechny moduly mimo Accounting.

NetEnforcer AC201

Do 10 Mbps,
12000současných spojení.
Volitelně všechny moduly.

NetEnforcer AC301

Do 100 Mbps,
64000 současných spojení.
Volitelně všechny moduly.

Allot Communications

NetEnforecer

1 U High

19” Rack Mount

Java-based GUI

Auto By-Pass

Full Redundancy

Traffic Shaping

Monitoring

Access Control

TOS Gateway

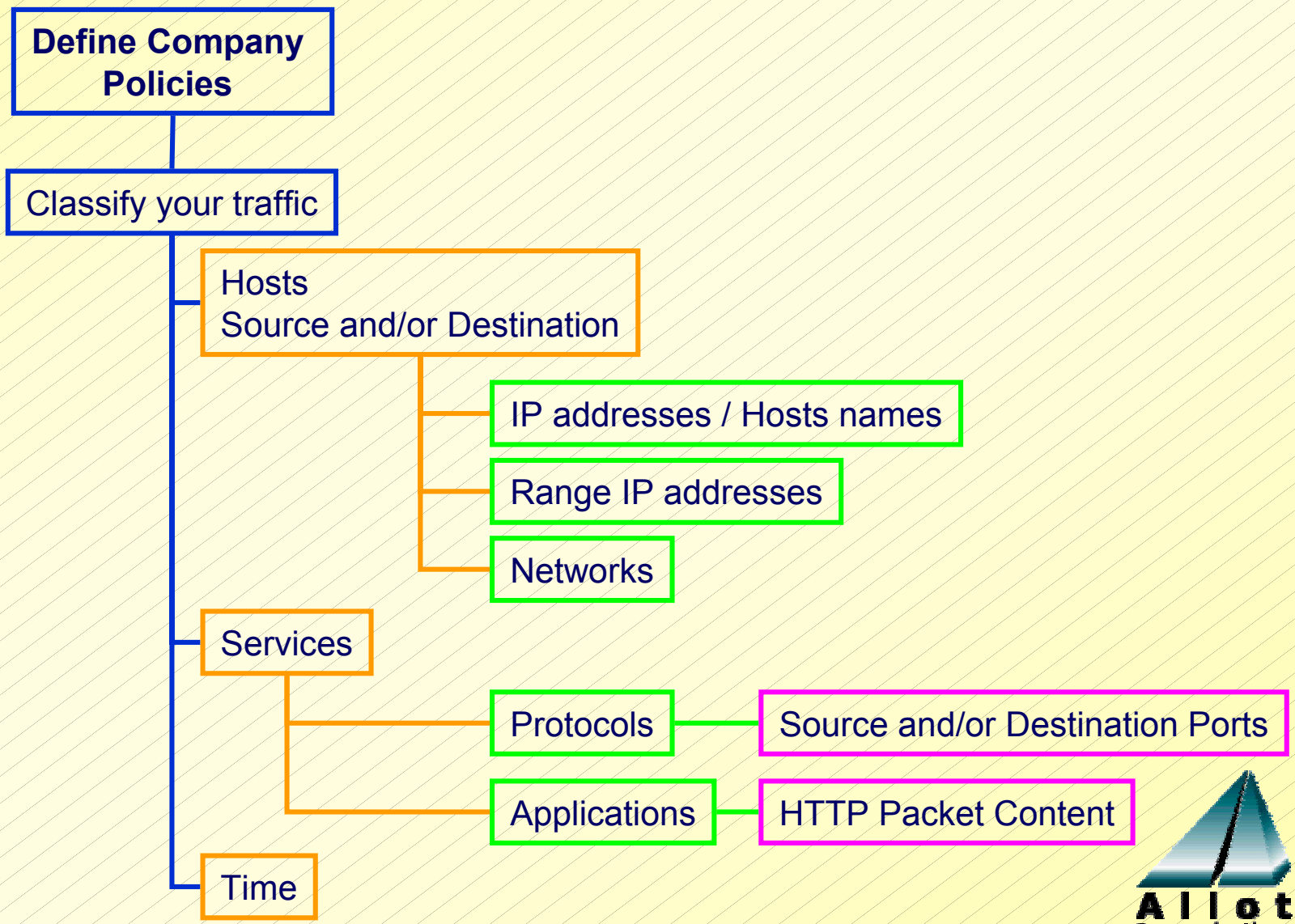
Accounting

Cache Enforcer

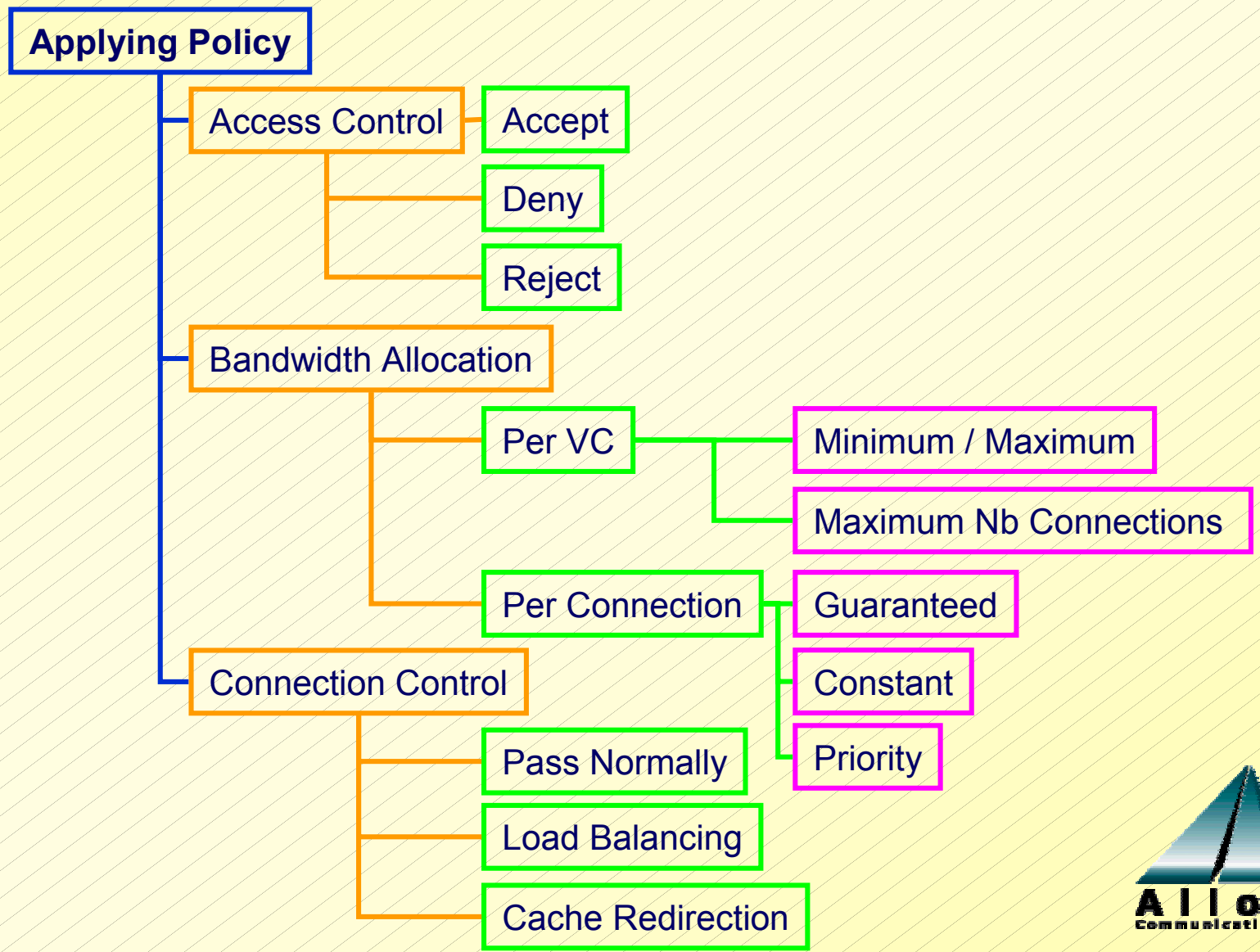
Load Balancing

Allot Communications

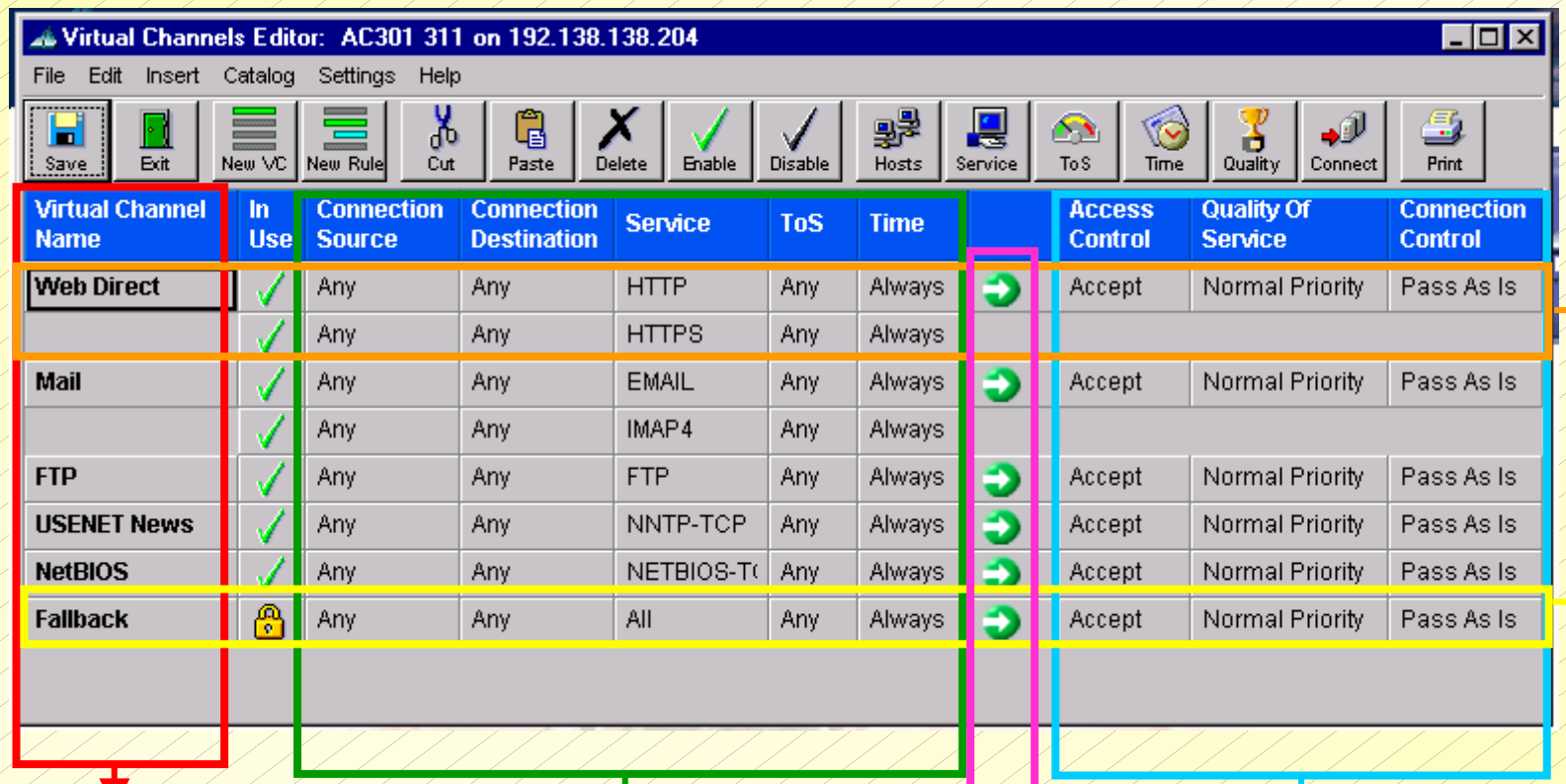
Kriteria pro vytváření pravidel



Vytváření pravidel



Virtual Channels Editor



One VC with 2 rules

FallBack

VC Names

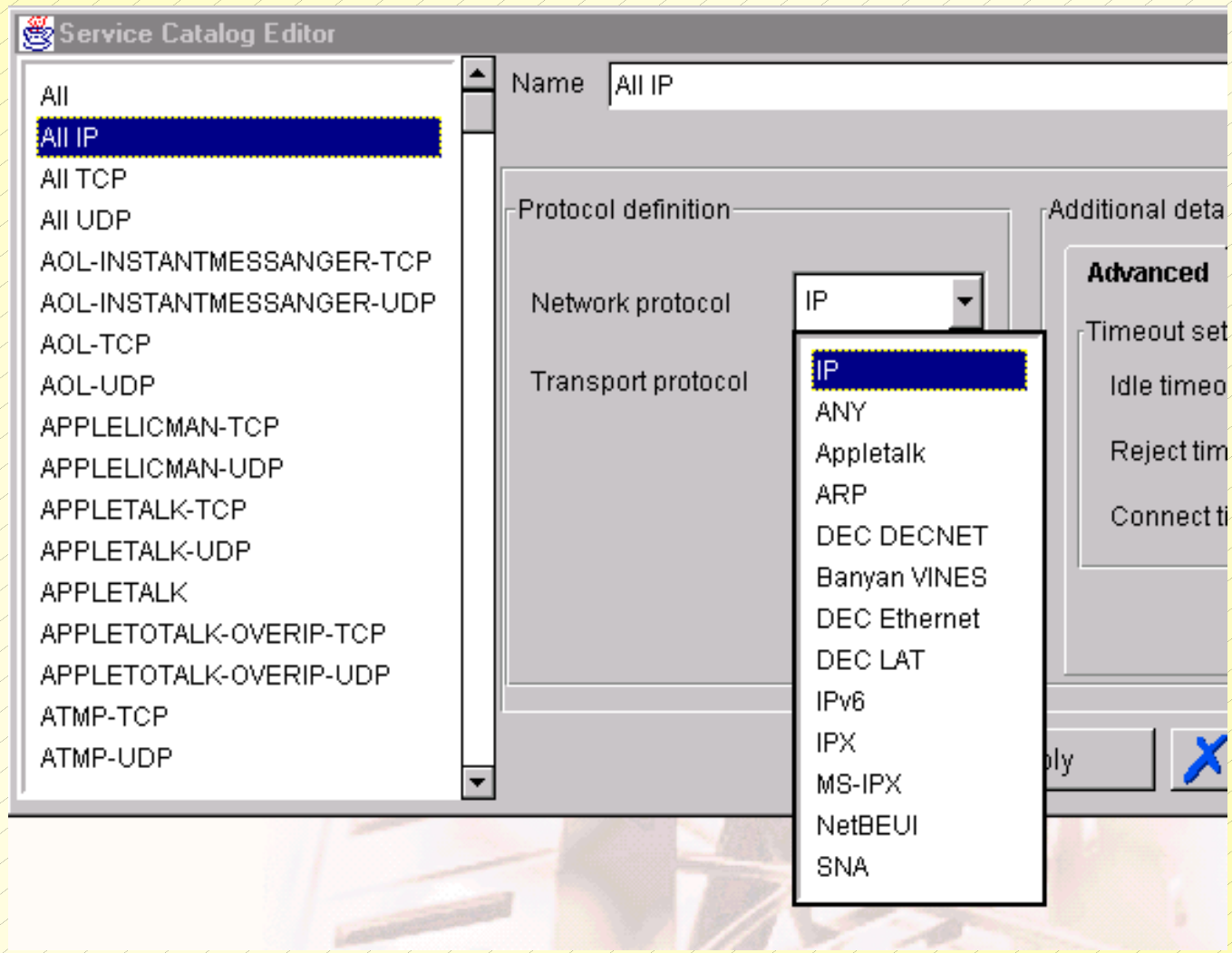
Rules (traffic Classification)

Expand Feature

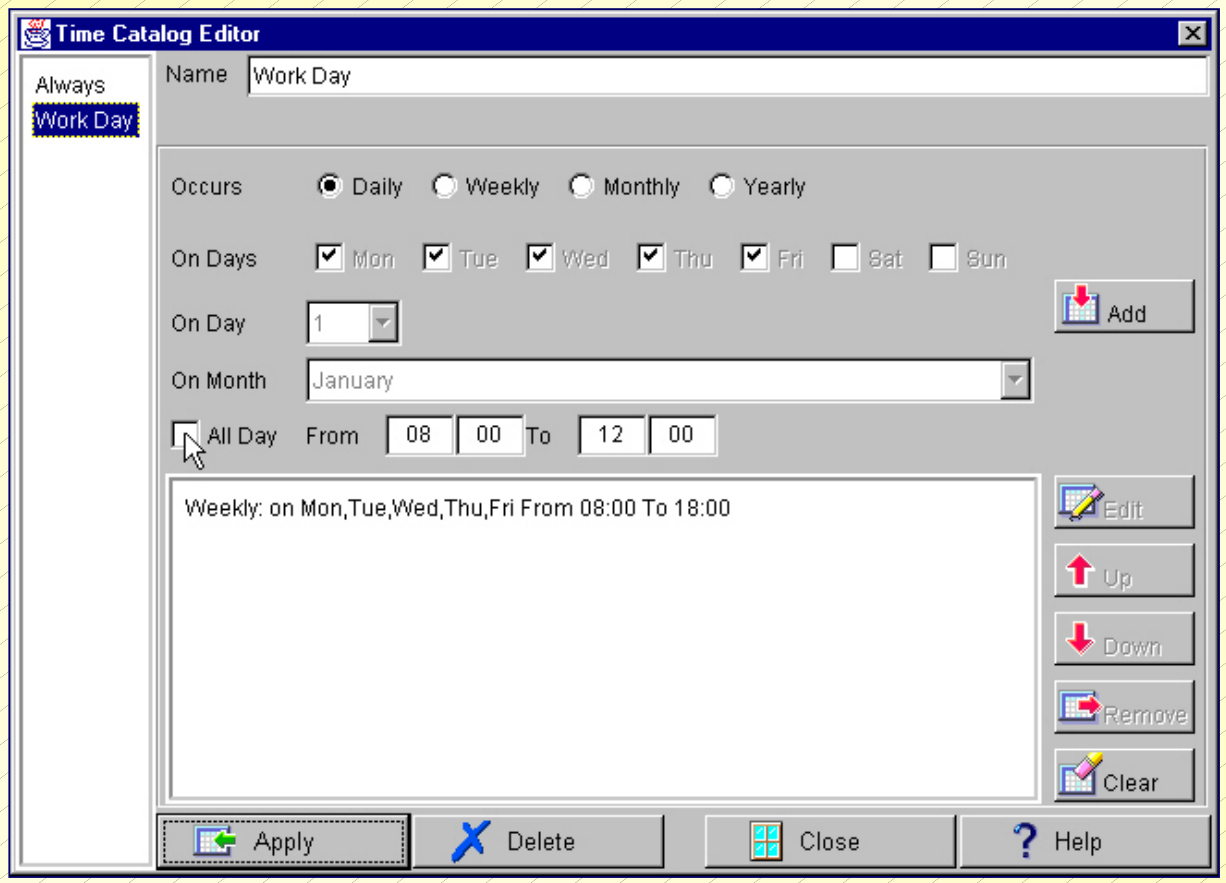
Policy actions

Allot Communications

Service Catalog



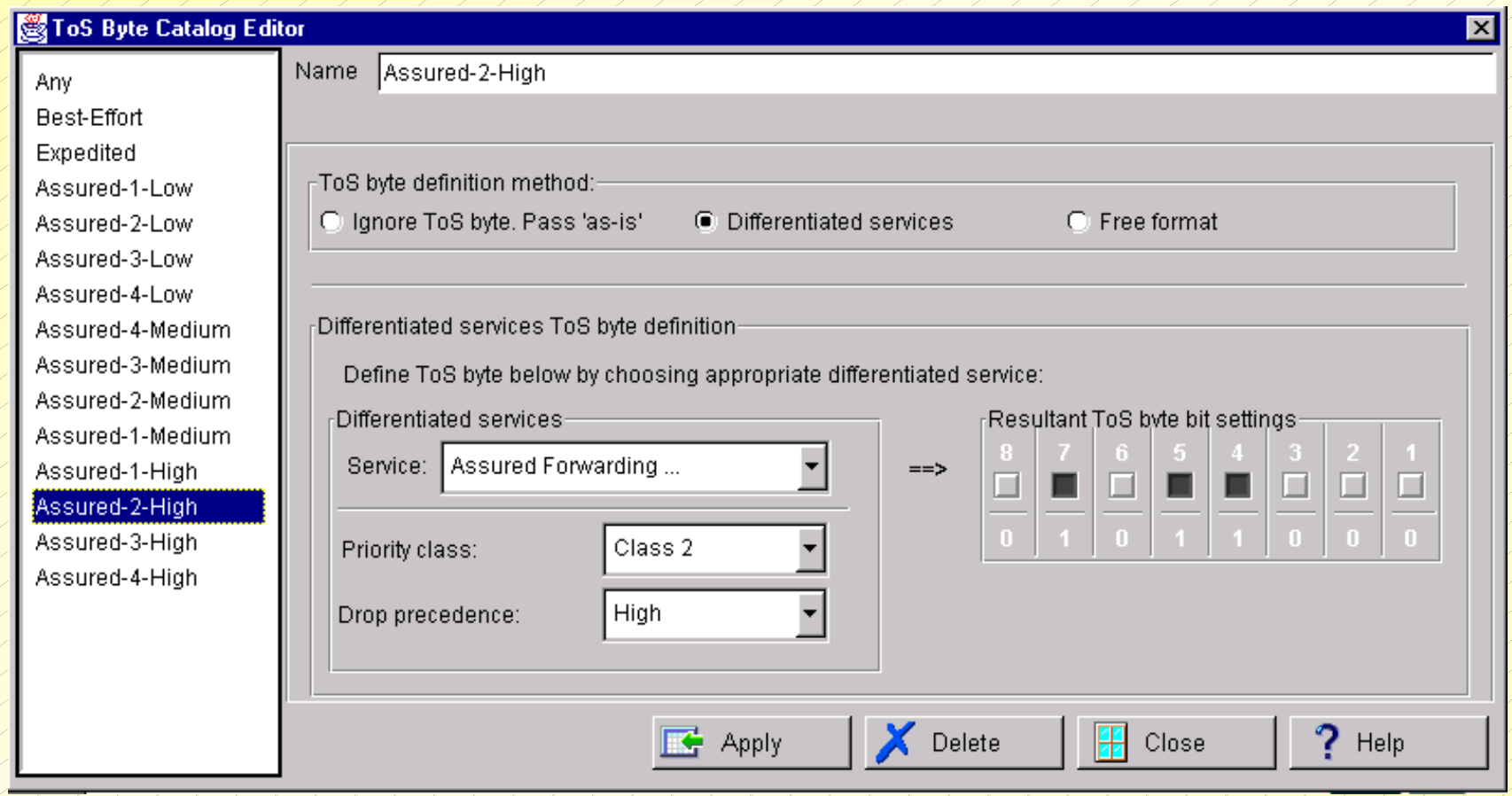
Time Catalog



Časové údaje

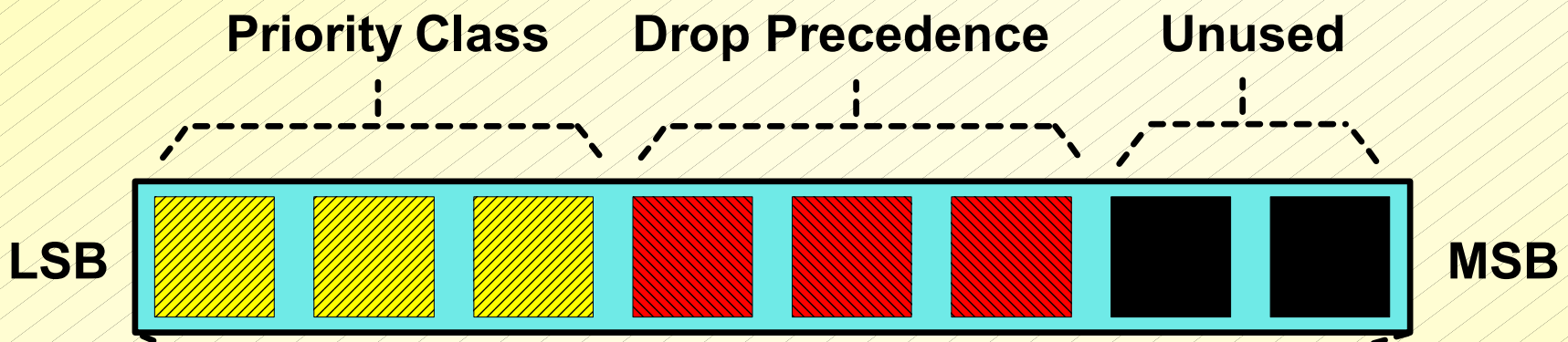
Allot Communications

TOS Catalog



Allot Communications

TOS (Type Of Service) a Diffserv



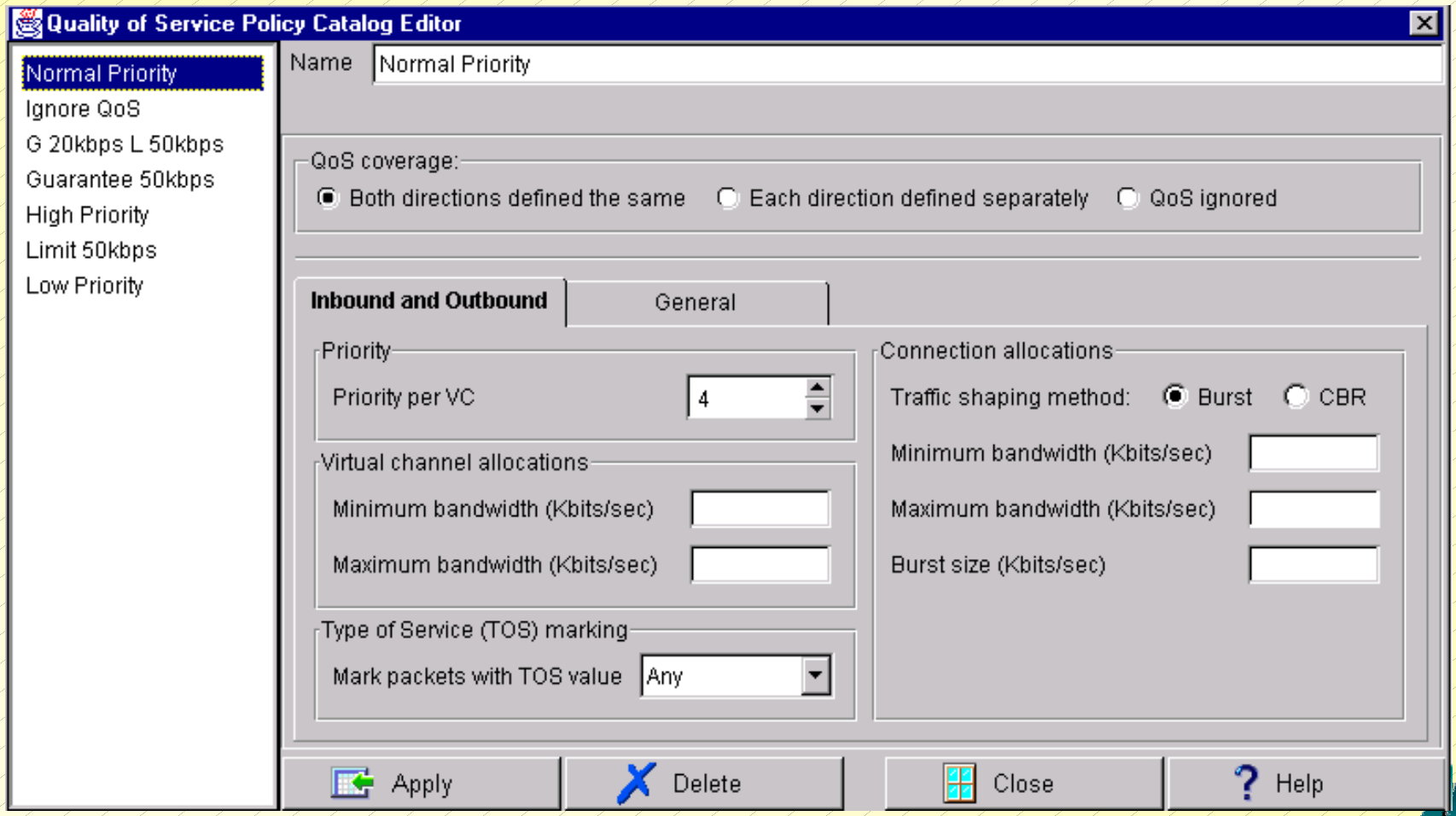
TOS Byte

Ver.	IHL	Type of service	Total length	
Identification			Flags	Fragment offset
Time to live		Protocol	Header checksum	
Source address				
Destination address				
Option + Padding				
Data				

IP Packet

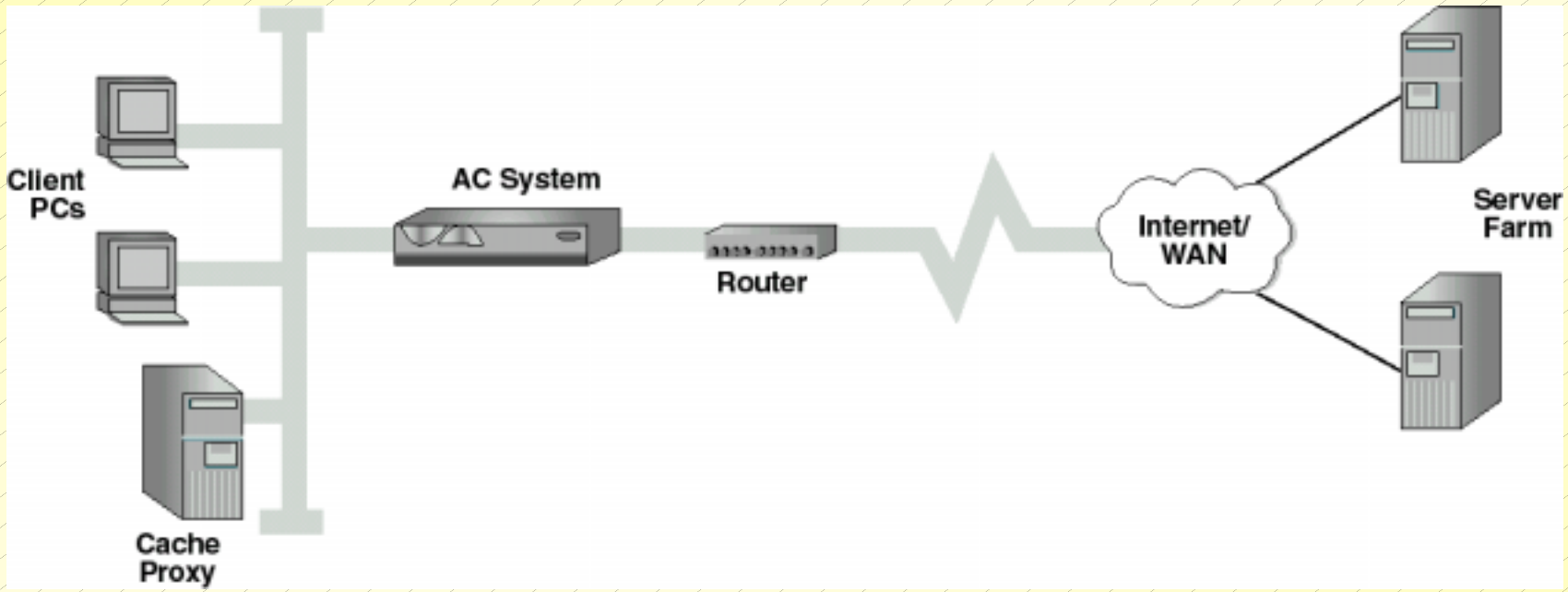
Allot Communications

Quality of Service

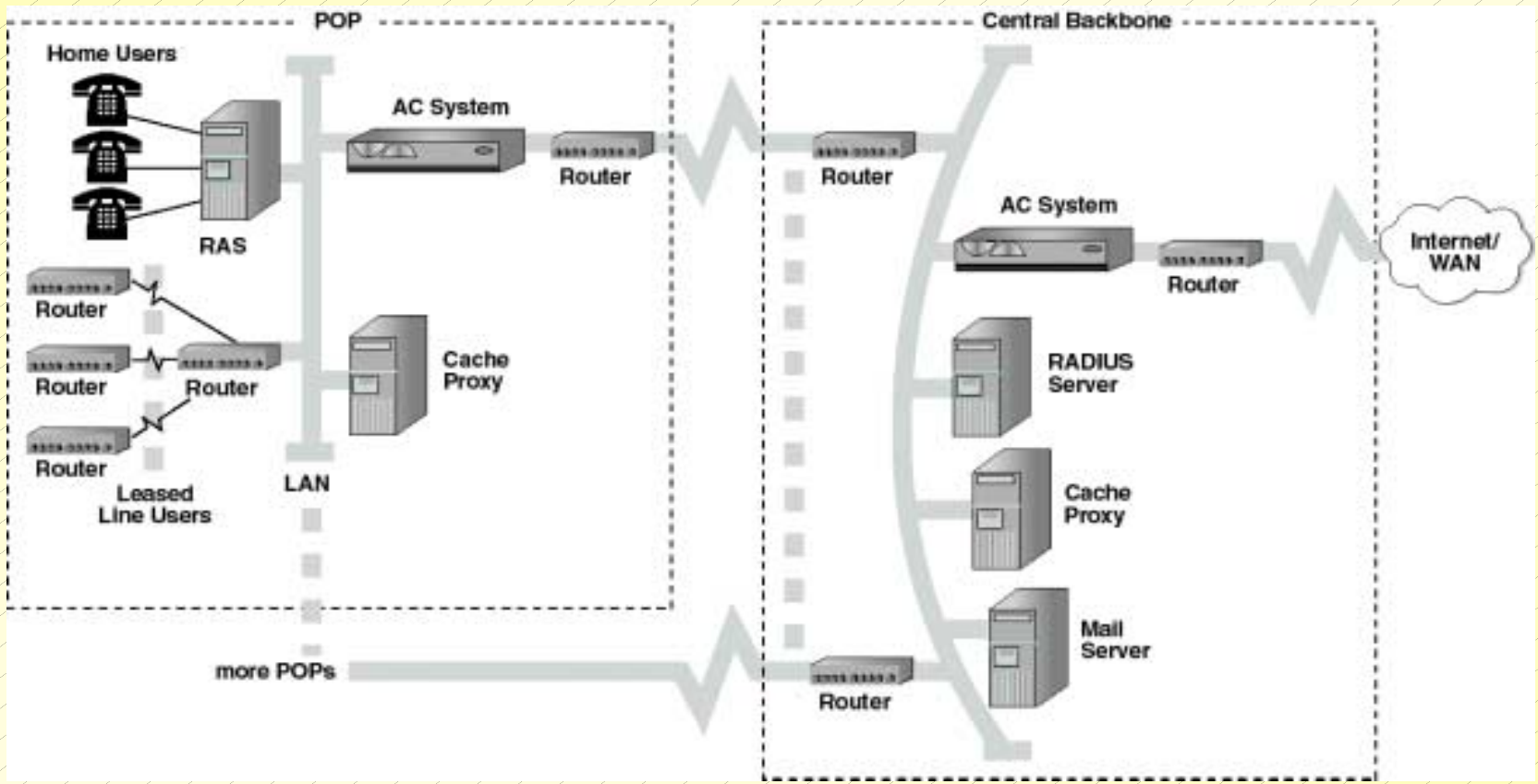


Allot Communications

Aplikace – podniková síť



Aplikace – síť ISP



Aplikce - webhosting

Up Link

Switch

10Mbps to Site 1

2Mbps to Site 2

20Mbps to Site 3

1Mbps to Site 4

Je garantována dostupnost!!

Site 1

Site 2

Site 3

Site 4

10Mbps-15Mbps to Server 1

3Mbps to Server 2

5Mbps to Server 3

10Mbps to Server 4

Allot Communications