

# Policy Based Networking = cesta jak zajistit QoS

**Petr Lasek**

VUMS DataCom

---



22.3.2001

Konference vysokorychlostní sítě



[www.datacom.cz](http://www.datacom.cz)



[www.allot.com](http://www.allot.com)

# Rychlost = kvalita služeb?



# Parametry ovlivňující QoS

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

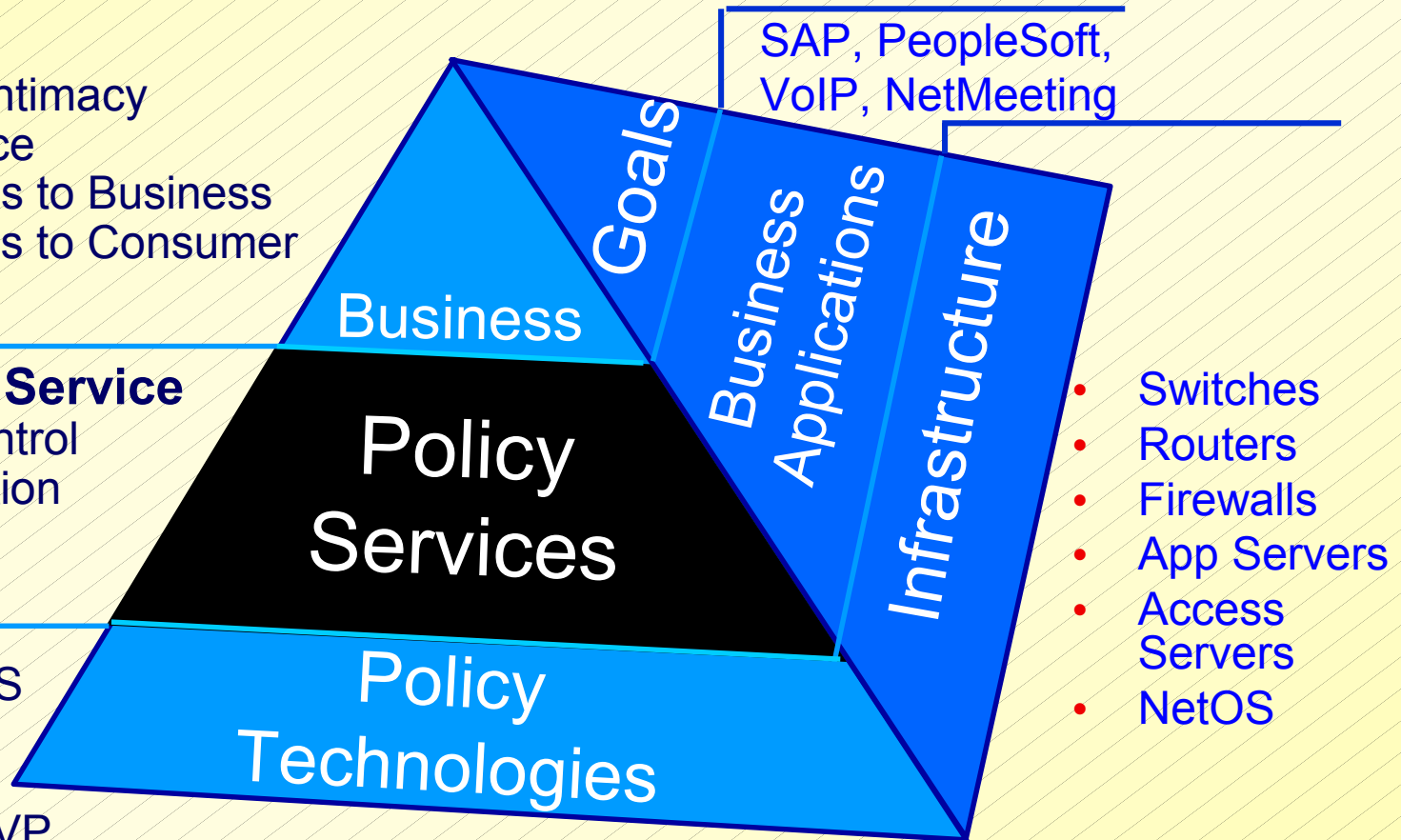


# Policy<sup>\*)</sup>-based Networking

- 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



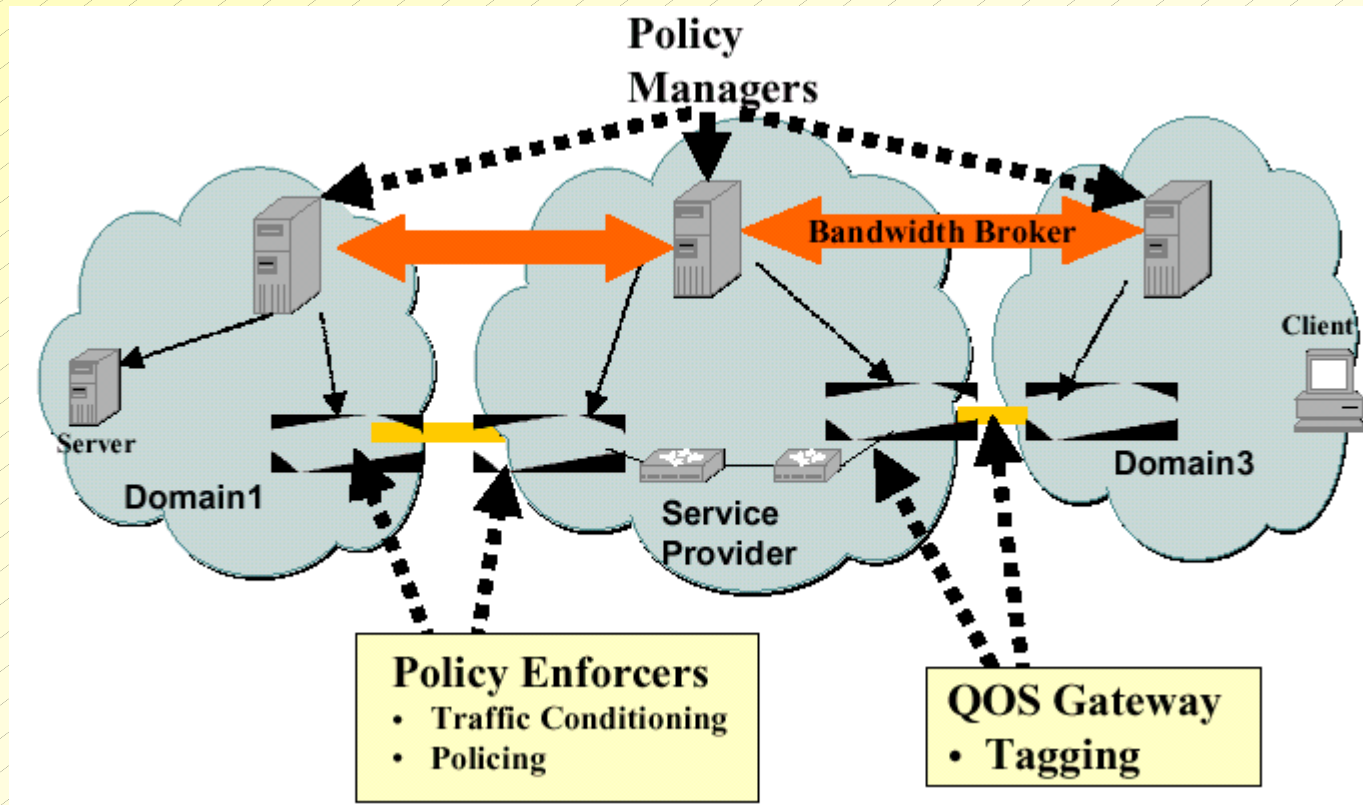
- Switches
- Routers
- Firewalls
- App Servers
- Access Servers
- NetOS



**\*) postup, taktika, plán, metoda, politika**



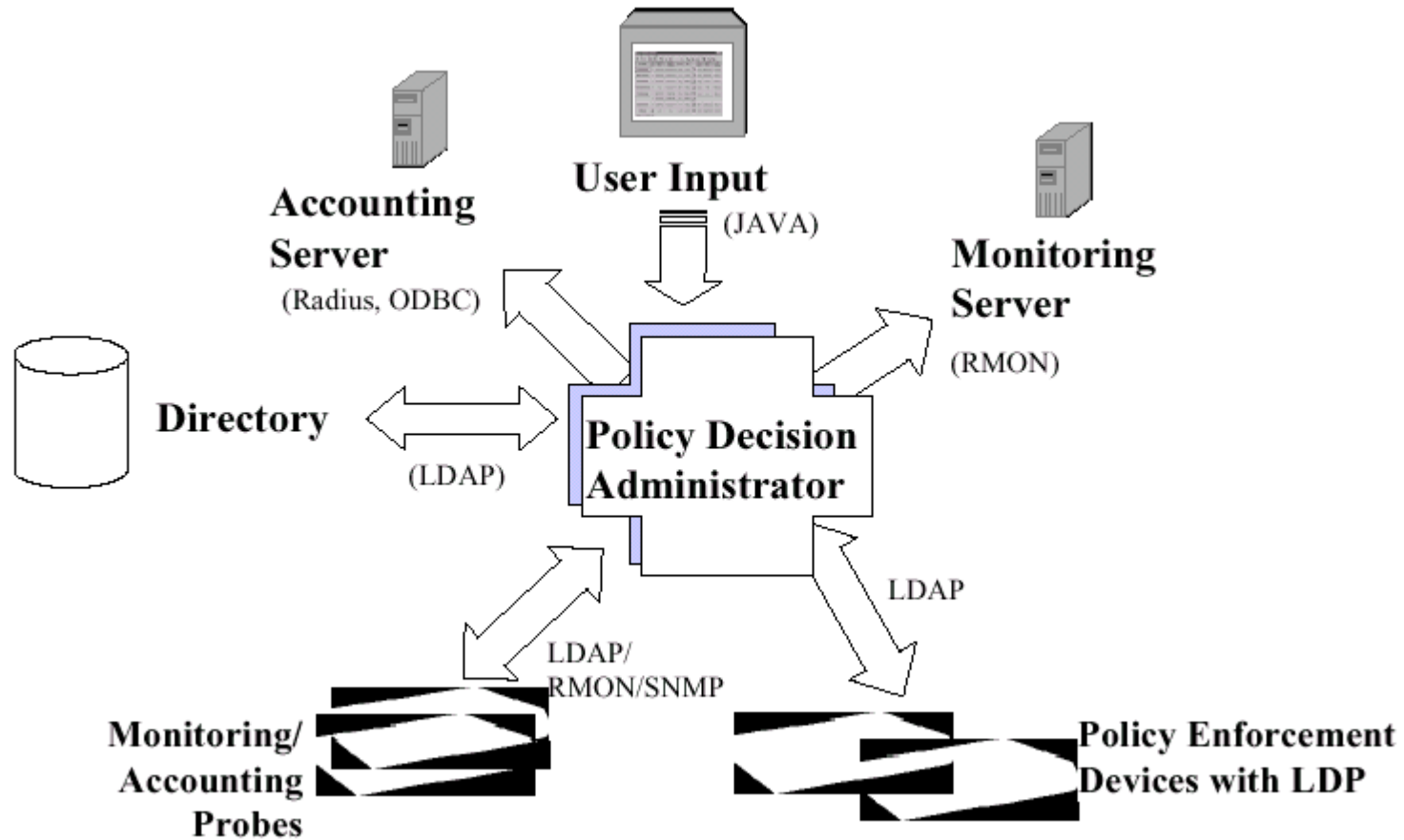
# Architektura



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



# Policy Management



Data Abstraction Layer  
Device Abstraction Layer



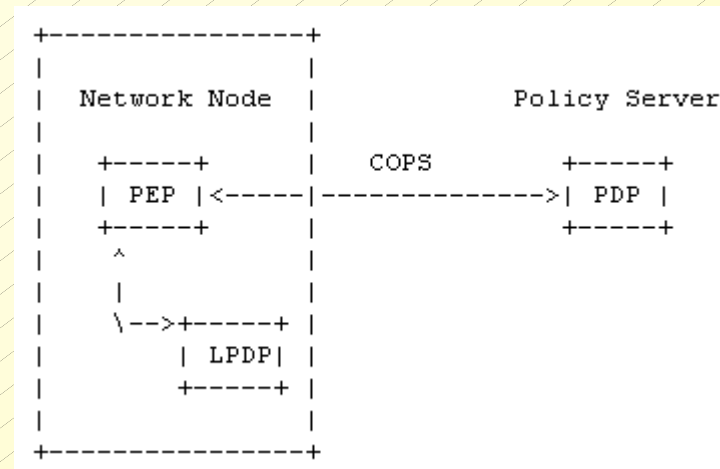
# CIM (Common Information Modul)

- „Taxonomie“ sítě
- Objektový model
- DMTF (Distributed 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





# 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

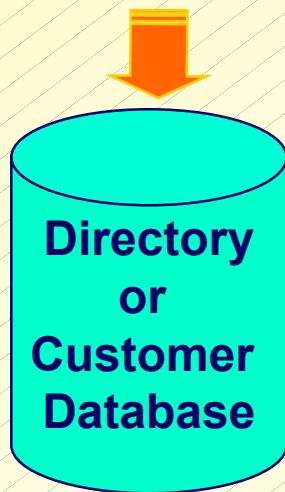
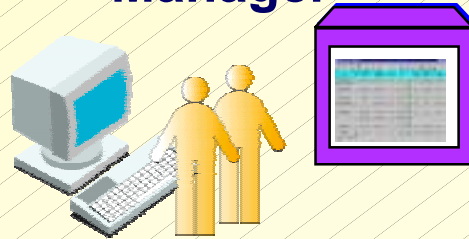
Access Control



# "Policy" Architektura

External  
Application  
Information

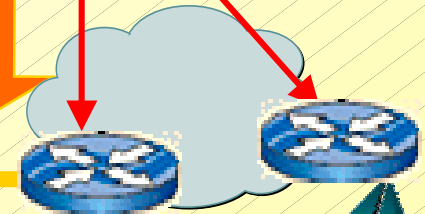
Network  
Manager



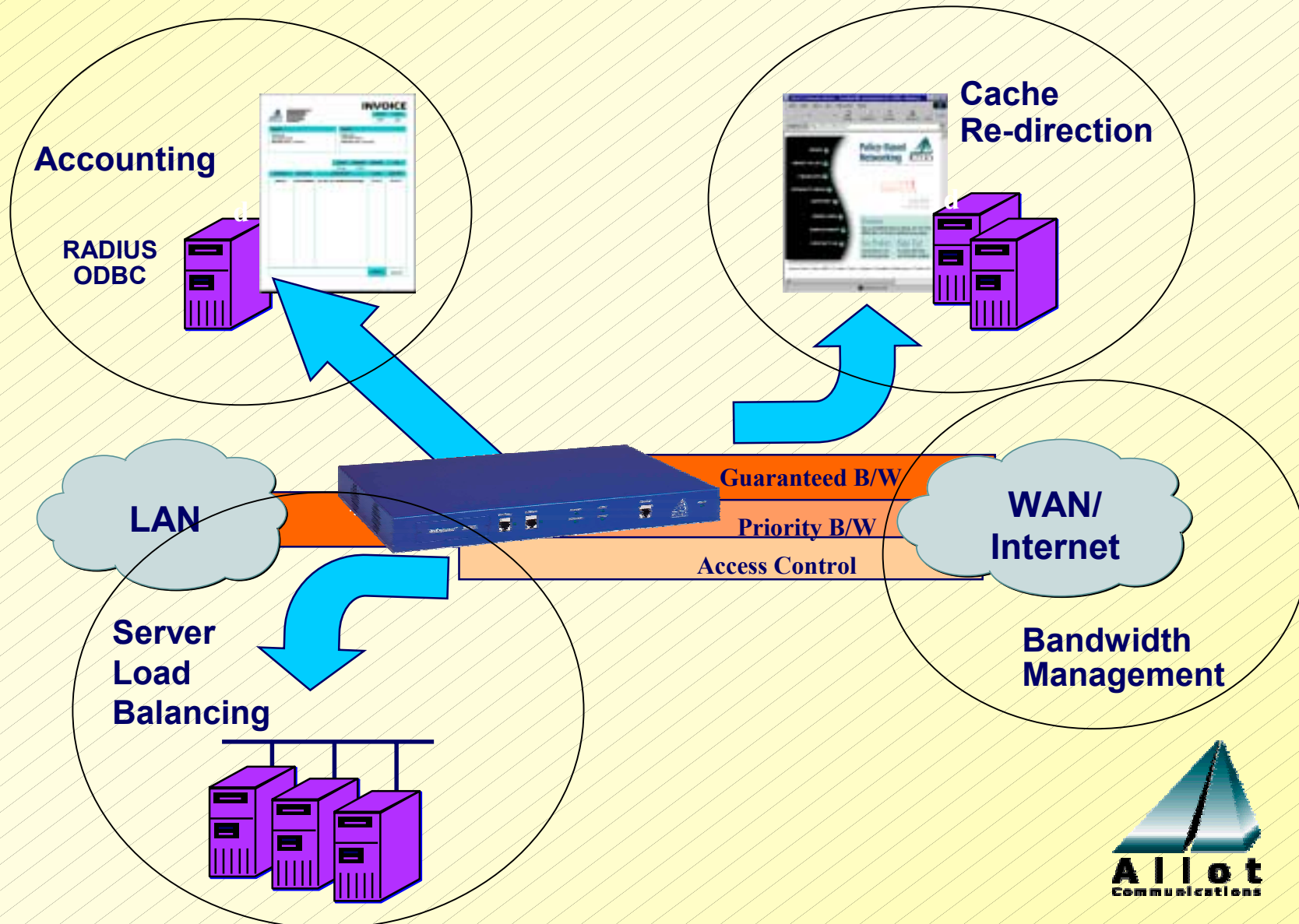
Enforcement Devices



Tag (Tos)



# The Solutions Family



# Allot Comprehensive Solution



## NetPolicy MANAGER

### Prosazování QoS

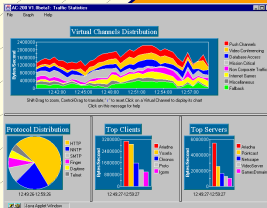
- Formování provozu (Traffic Shaping)
- Přidělování priorit
- Podmínky pro mission-critical aplikace
- Garantování SLA
- QoS Tagging

### 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



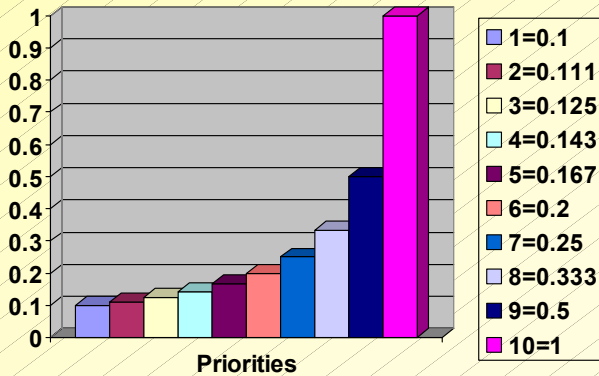
# Quality of Service

- 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

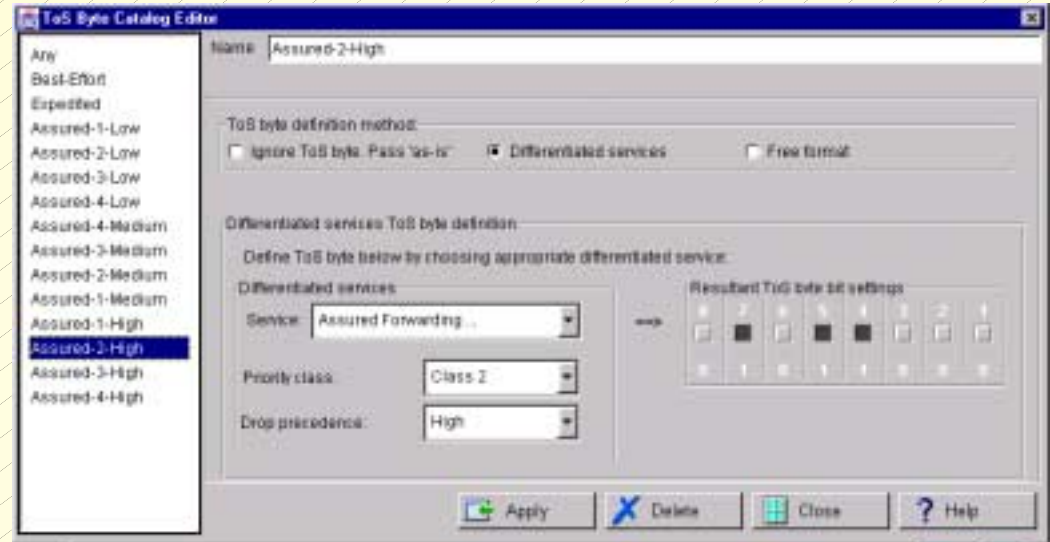


# Quality of Service

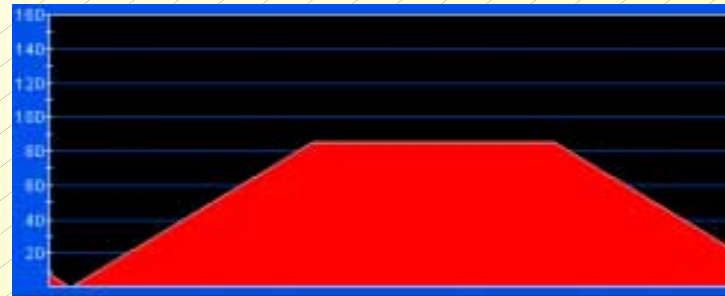
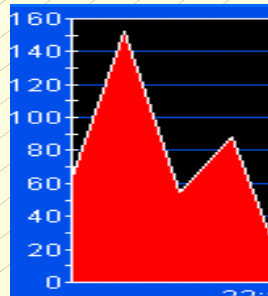
## Priority (10)



## TOS

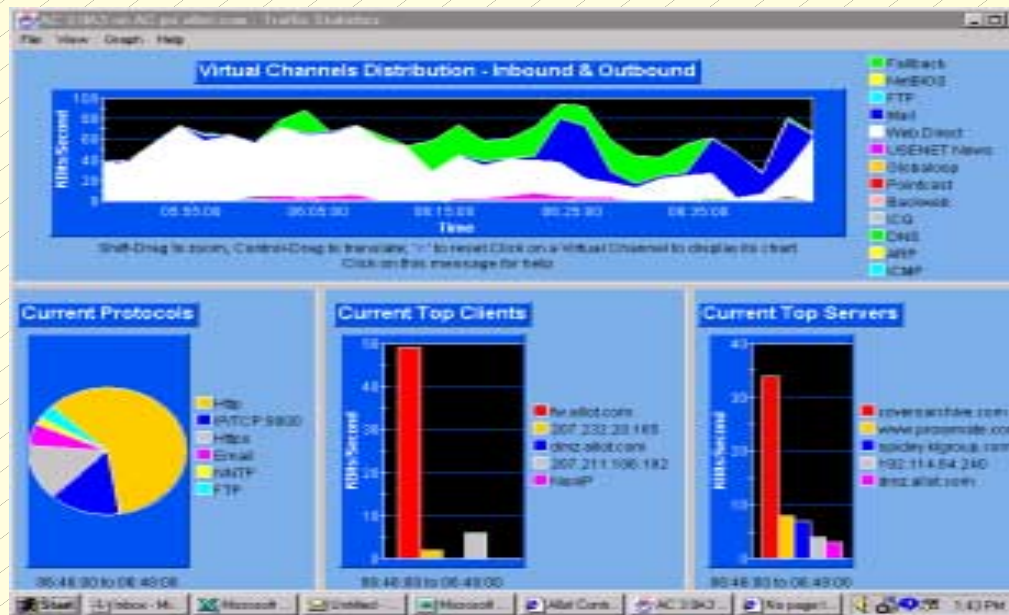


## CIR/MIR



# Monitoring

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



# Load-Balancing

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





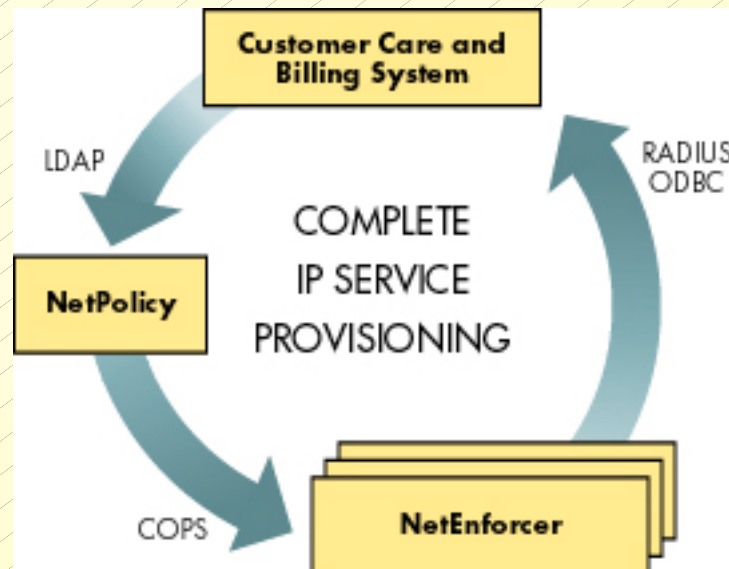
# Cache Redirection

- 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,  
12000 současných spojení.  
Volitelně všechny moduly.



**NetEnforcer AC301**

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

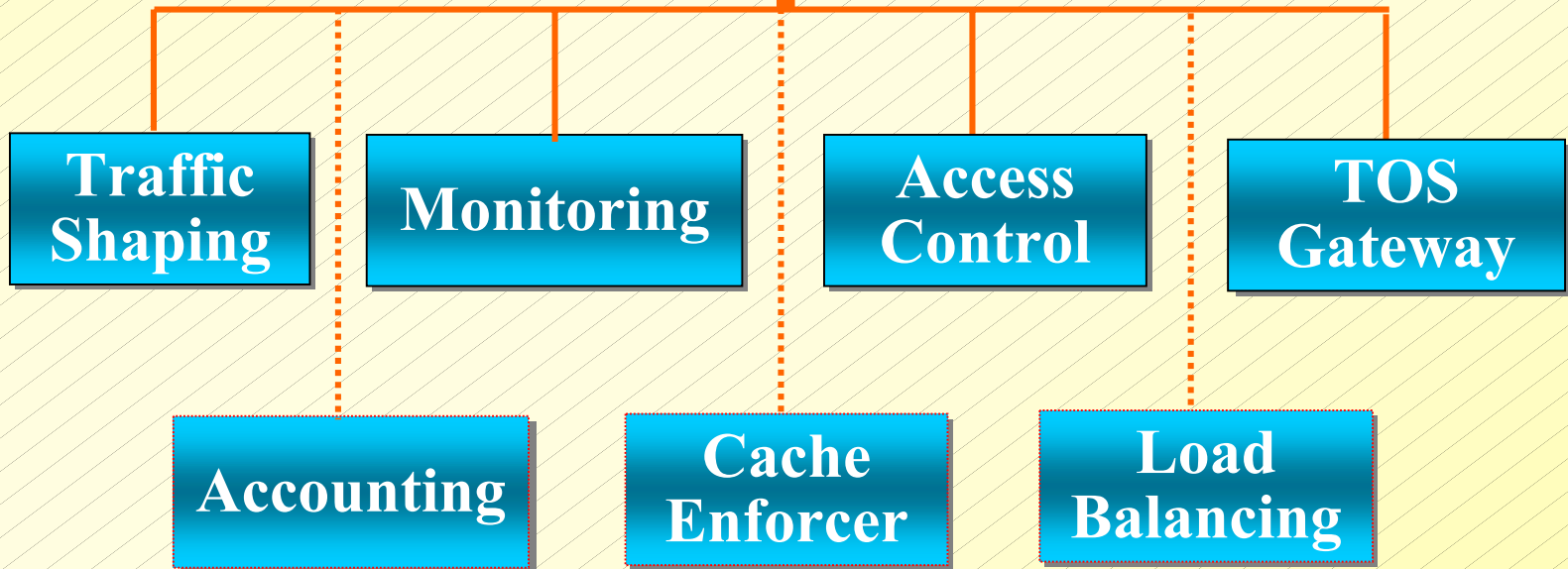


# NetEnforecer

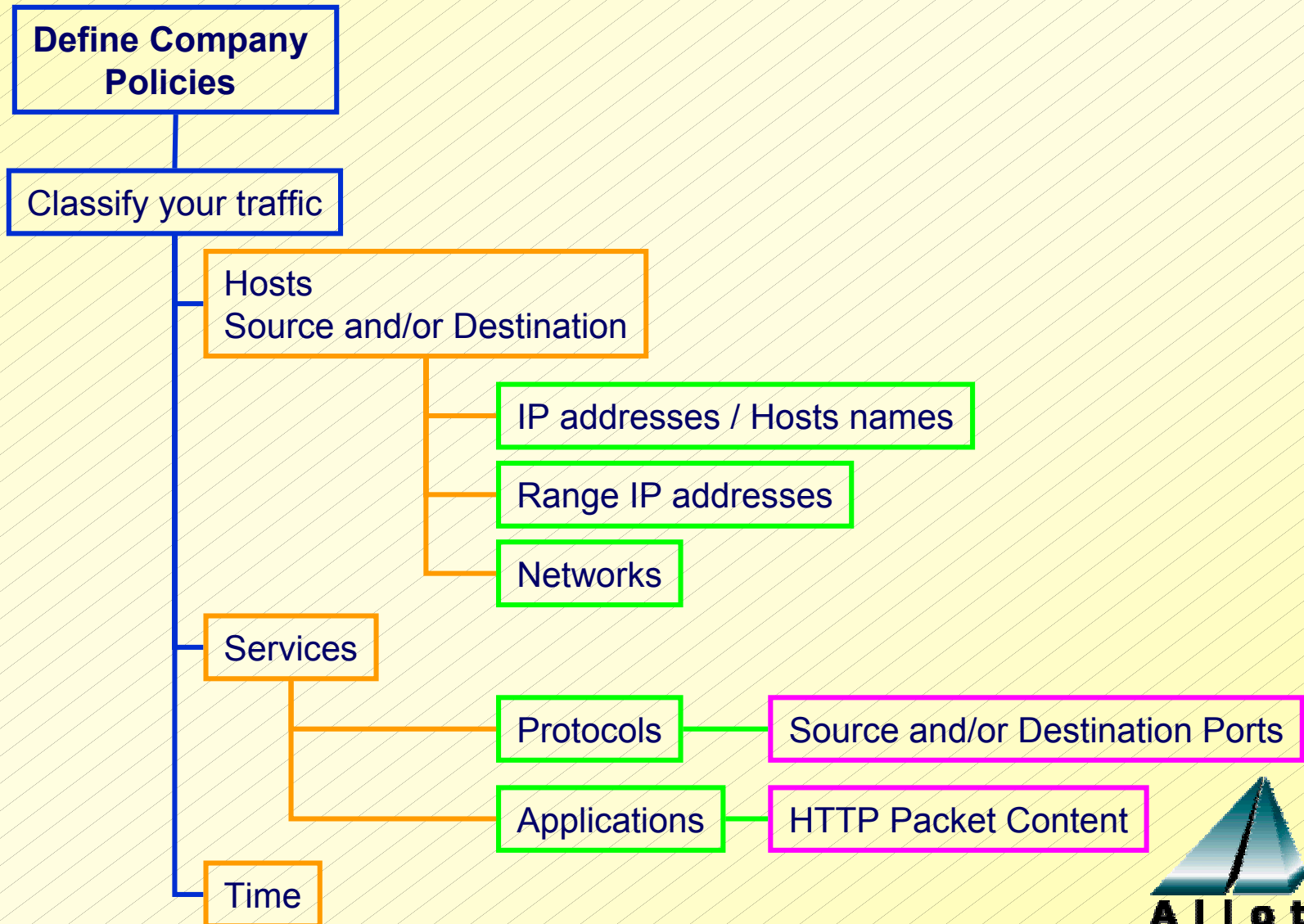
**1 U High**  
**19" Rack Mount**



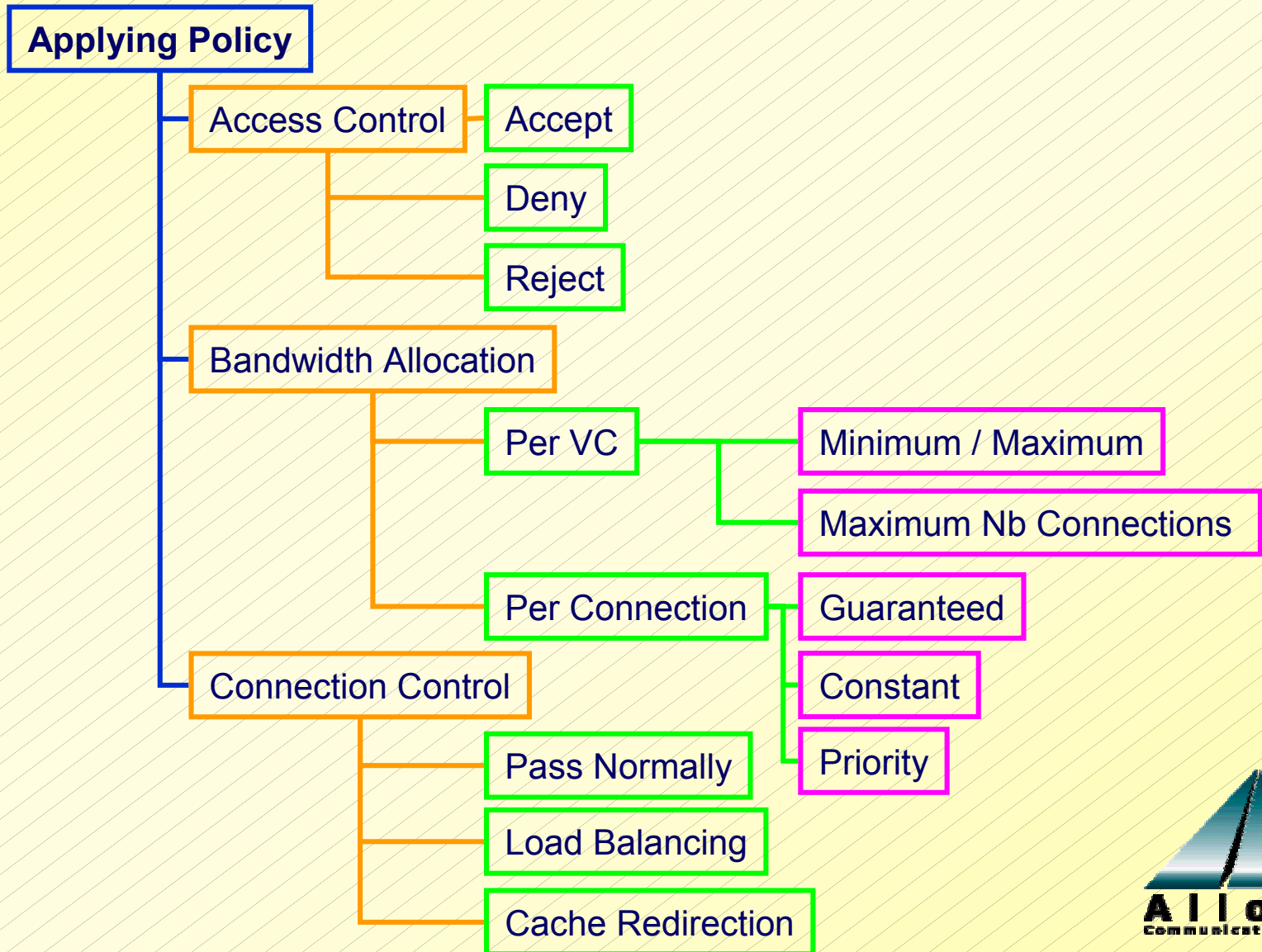
**Java-based GUI**  
**Auto By-Pass**  
**Full Redundancy**



# Kriteria pro vytváření pravidel



# Vytváření pravidel



# Virtual Channels Editor

Virtual Channels Editor: AC301 311 on 192.138.138.204

File Edit Insert Catalog Settings Help

Save Exit New VC New Rule Cut Paste Delete Enable Disable Hosts Service ToS Time Quality Connect Print

Virtual Channel Name	In Use	Connection Source	Connection Destination	Service	ToS	Time		Access Control	Quality Of Service	Connection Control
Web Direct	✓	Any	Any	HTTP	Any	Always	➔	Accept	Normal Priority	Pass As Is
	✓	Any	Any	HTTPS	Any	Always				
Mail	✓	Any	Any	EMAIL	Any	Always	➔	Accept	Normal Priority	Pass As Is
	✓	Any	Any	IMAP4	Any	Always				
FTP	✓	Any	Any	FTP	Any	Always	➔	Accept	Normal Priority	Pass As Is
USENET News	✓	Any	Any	NNTP-TCP	Any	Always	➔	Accept	Normal Priority	Pass As Is
NetBIOS	✓	Any	Any	NETBIOS-Tc	Any	Always	➔	Accept	Normal Priority	Pass As Is
Fallback	🔒	Any	Any	All	Any	Always	➔	Accept	Normal Priority	Pass As Is

One VC with 2 rules

Fallback

VC Names

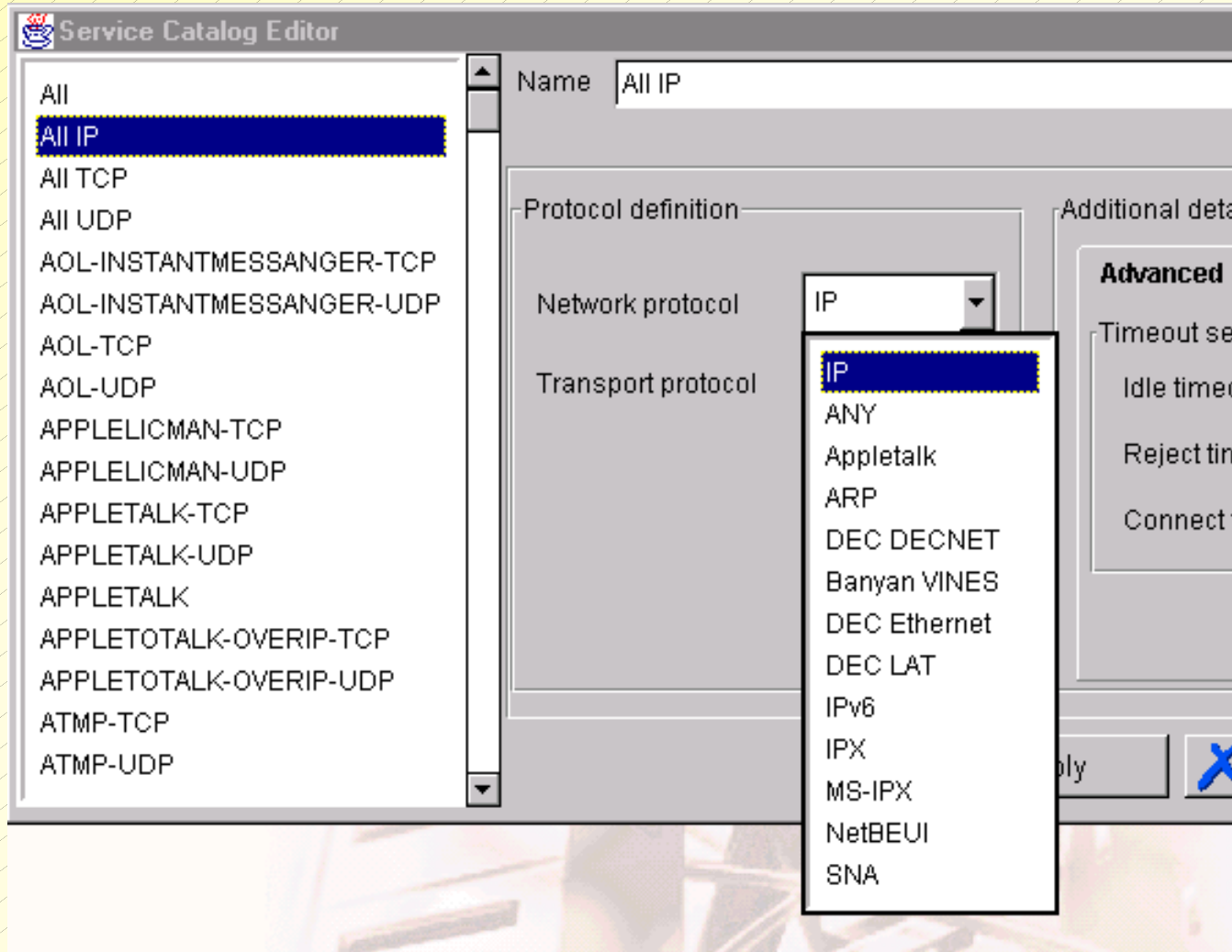
Rules (traffic Classification)

Policy actions

Expand Feature



# Service Catalog





# Time Catalog

The screenshot shows the 'Time Catalog Editor' window. The title bar reads 'Time Catalog Editor'. On the left, there is a sidebar with two items: 'Always' and 'Work Day', with 'Work Day' selected. The main area contains the following fields and controls:

- Name:** Work Day
- Occurs:** Radio buttons for Daily (selected), Weekly, Monthly, and Yearly.
- On Days:** Checkboxes for Mon, Tue, Wed, Thu, Fri (all checked), Sat, and Sun (unchecked).
- On Day:** A dropdown menu showing '1'.
- On Month:** A dropdown menu showing 'January'.
- All Day:** An unchecked checkbox.
- From:** Time input fields showing '08' and '00'.
- To:** Time input fields showing '12' and '00'.
- Summary:** A text box containing 'Weekly: on Mon,Tue,Wed,Thu,Fri From 08:00 To 18:00'.

On the right side of the main area, there are several buttons: 'Add', 'Edit', 'Up', 'Down', 'Remove', and 'Clear'. At the bottom of the window, there are four buttons: 'Apply', 'Delete', 'Close', and 'Help'.

Časové údaje



# TOS Catalog

**ToS Byte Catalog Editor**

Name: Assured-2-High

ToS byte definition method:

Ignore ToS byte. Pass 'as-is'     Differentiated services     Free format

Differentiated services ToS byte definition

Define ToS byte below by choosing appropriate differentiated service:

Differentiated services

Service: Assured Forwarding ... ==>

Priority class: Class 2

Drop precedence: High

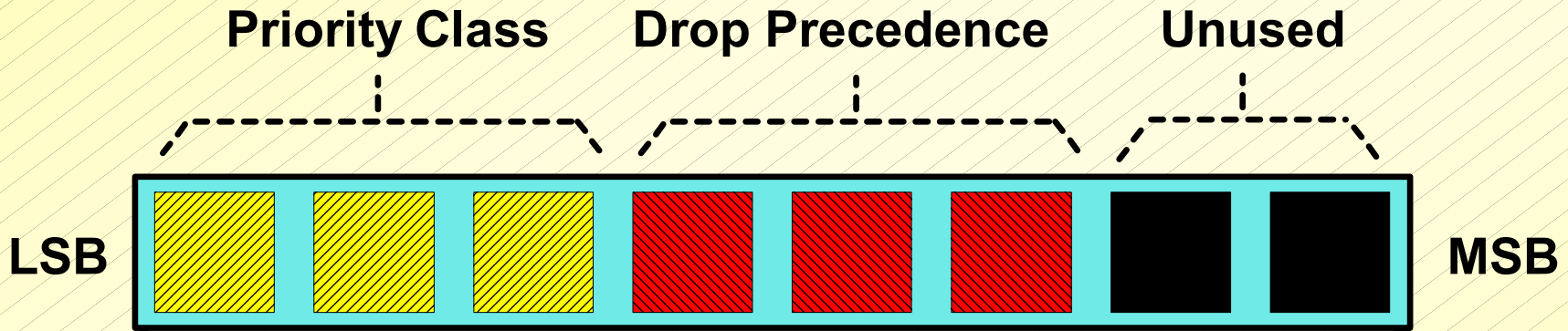
Resultant ToS byte bit settings

8	7	6	5	4	3	2	1
<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
0	1	0	1	1	0	0	0

Apply    Delete    Close    Help



# 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



# Quality of Service

**Quality of Service Policy Catalog Editor**

Name: Normal Priority

QoS coverage:  
 Both directions defined the same    Each direction defined separately    QoS ignored

**Inbound and Outbound**   **General**

Priority:  
Priority per VC: 4

Virtual channel allocations:  
Minimum bandwidth (Kbits/sec):  
Maximum bandwidth (Kbits/sec):

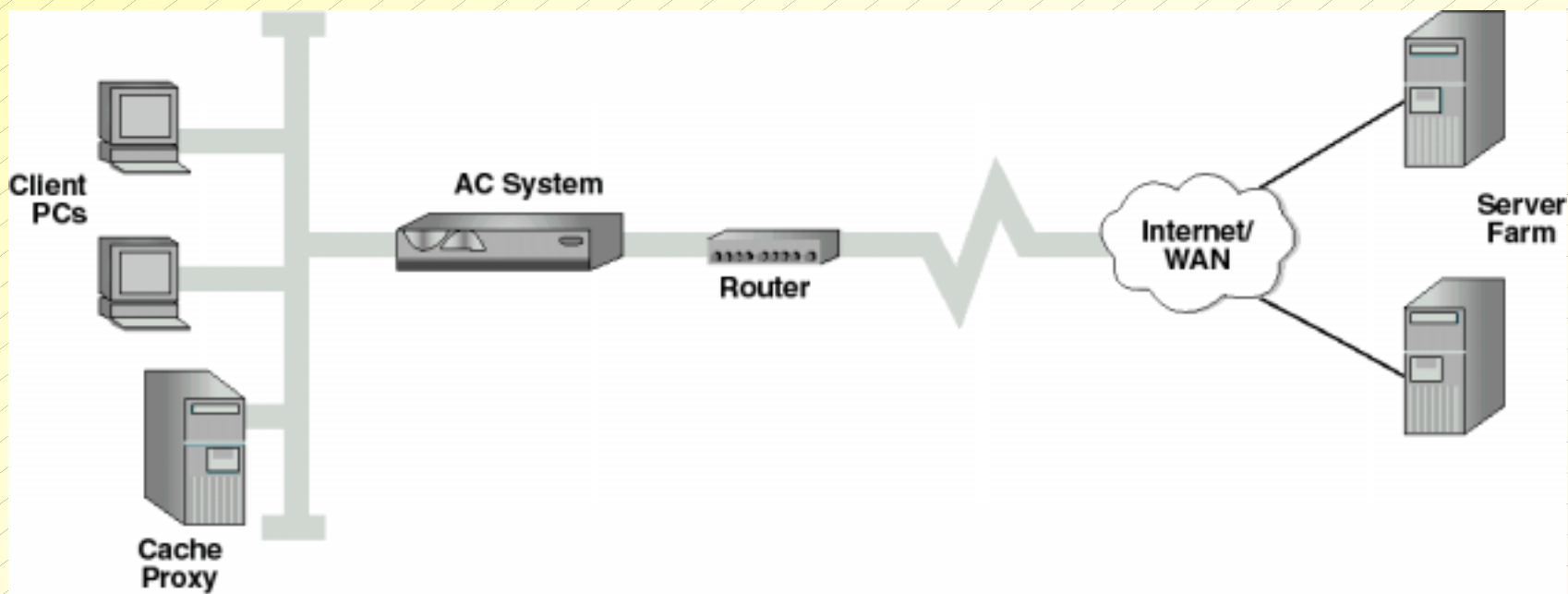
Type of Service (TOS) marking:  
Mark packets with TOS value: Any

Connection allocations:  
Traffic shaping method:  Burst    CBR  
Minimum bandwidth (Kbits/sec):  
Maximum bandwidth (Kbits/sec):  
Burst size (Kbits/sec):

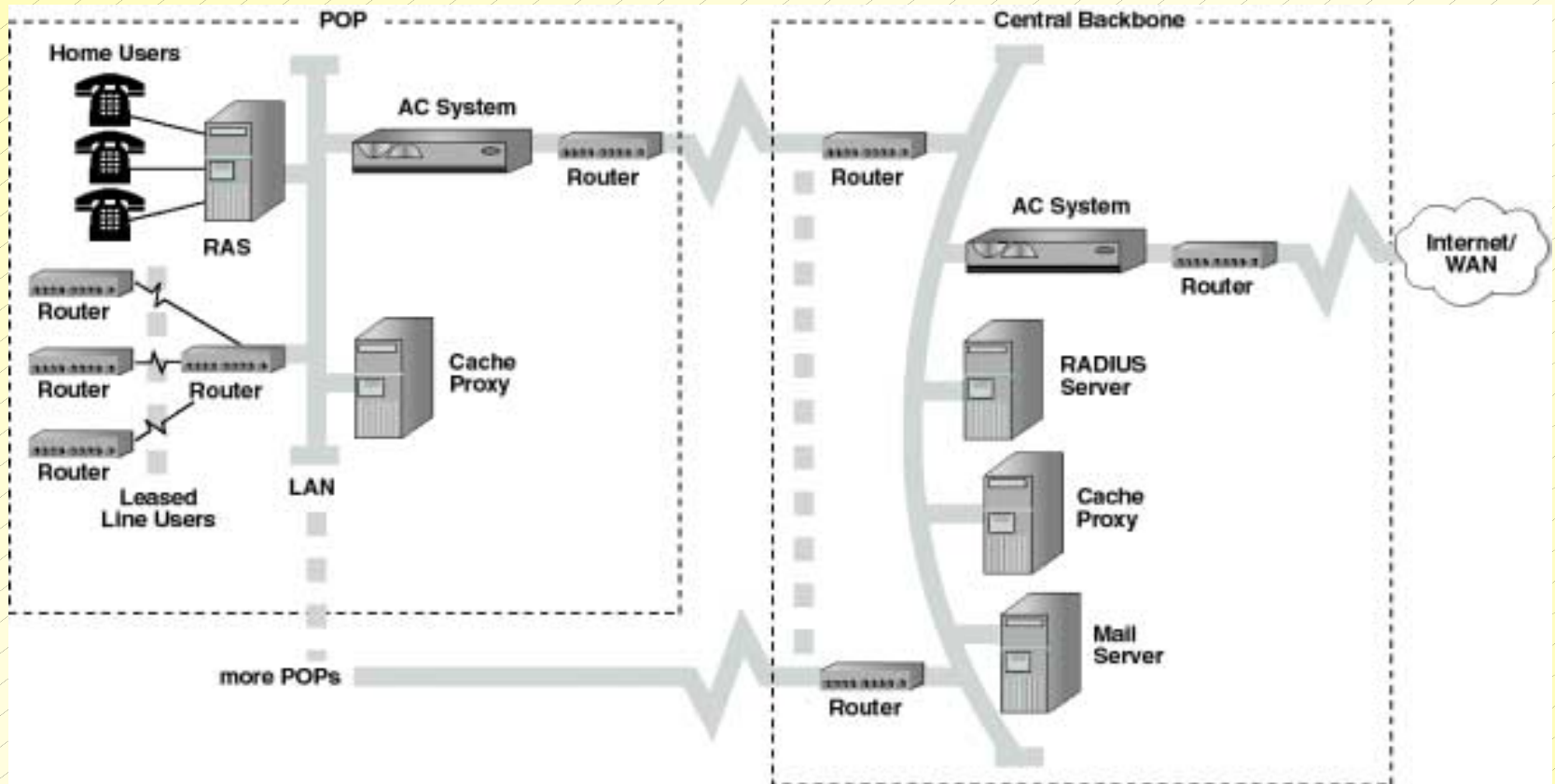
Apply   Delete   Close   Help



# Aplikace – podniková síť



# Aplikace – síť ISP



# Aplikce - webhosting



Up Link

Switch

