


**Boundless
Communications**



Outbound QoS Server “Allot NetXplorer”

This presentation constitutes proprietary and confidential information of Gilat Satellite Networks Ltd. This presentation may not be disclosed, used or duplicated, in whole or in part, without the prior written consent of Gilat Satellite Networks Ltd.

This document contains information proprietary to Gilat Satellite Networks Ltd. and may not be reproduced in whole or in part without the express written consent of Gilat Satellite Networks Ltd. The disclosure by Gilat Satellite Networks Ltd. of information contained herein does not constitute any license or authorization to use or disclose the information, ideas or concepts presented. The contents of this document are subject to change without prior notice.



Session Objectives



- **General Description**
 - **NetXplorer Server**
 - **Monitoring**
 - **NetEnforcer**
 - **Hardware Description**
 - **Active Redundancy**
 - **Bypass Mode**
 - **Connectivity**
 - **NetXplorer GUI Client**
- **QoS Policy Configuration**
 - **Catalogs**
 - **Hierarchy Levels**
 - **Conditions**
 - **Actions**
- **Recommended Gilat Configuration**

Confidential and proprietary information



Allot QoS System

General Description

- **SkyEdge and SkyEdge II systems use the Allot System for the OB QoS needs**
 - **The Allot QoS system consists of three components:**
 - NetXplorer Server
 - Provides a centralized management system for all NetEnforcers of the network
 - NetEnforcer Units
 - Traffic shaping device that inspects and monitors network traffic
 - NetXplorer GUI Clients
 - Graphic User Interface client that runs on a Windows PC and uses Java



Allot System Components

System Specs

- Allot NetExplorer
 - Linux Red-Hat machine with RAID 1, 4 / 8GB RAM, and 500G hard drive
- Allot NetEnforcer

Model	Bandwidth	Lines	Pipes	VCs	Connections
AC502	45 - 200 Mbps FD	256	4,096	32,768	256,000

Confidential and proprietary information



Allot NetXplorer

- **The NetXplorer server is a centralized management platform**
 - **It is the actual application which includes the database and an integrated data collector**
 - **Manages and communicates with the different clients that access the system**
 - **Facilitates NetEnforcer configuration, policy provisioning, alarms**
 - **Monitoring and reporting**
 - Reports may be generated automatically in various formats
 - Real time traffic monitoring
 - For 4 hours (at 30 sec interval)
 - For up to 48 hours (at 5 min interval)
 - Long term traffic monitoring (requires license)
 - For 3 months (at 1 hour resolution)
 - For 1 year (at daily resolution)

Confidential and proprietary information

5

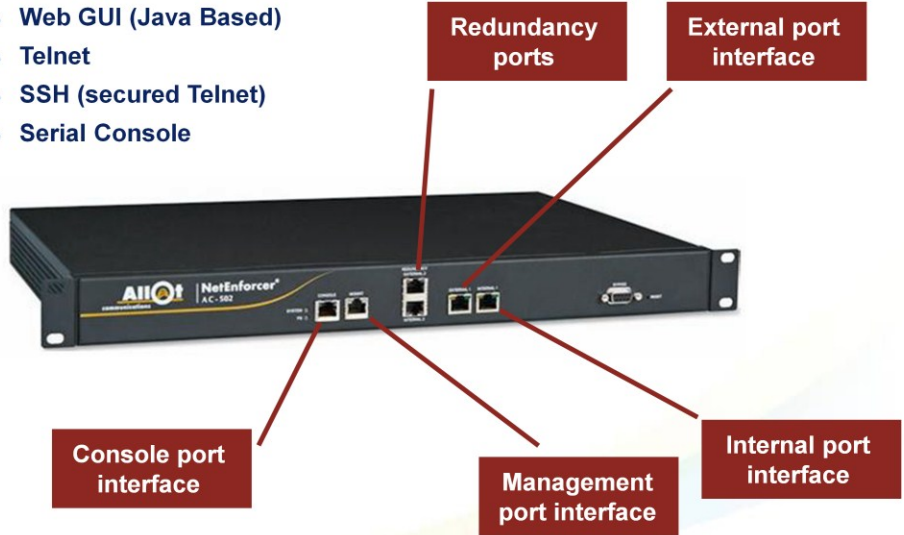


NetEnforcer AC-502 Hardware

Front Panel - Connectors

- **NetEnforcer Control and Management**

- Web GUI (Java Based)
- Telnet
- SSH (secured Telnet)
- Serial Console



Confidential and proprietary information

6

The dedicated Management port on the NetEnforcer enables out-of-band management of the device. Operating through the Management port increases security by denying access to the device via the Internal or External ports. Moreover, when there is a problem in the regular network it is still possible to manage and monitor the NetEnforcer

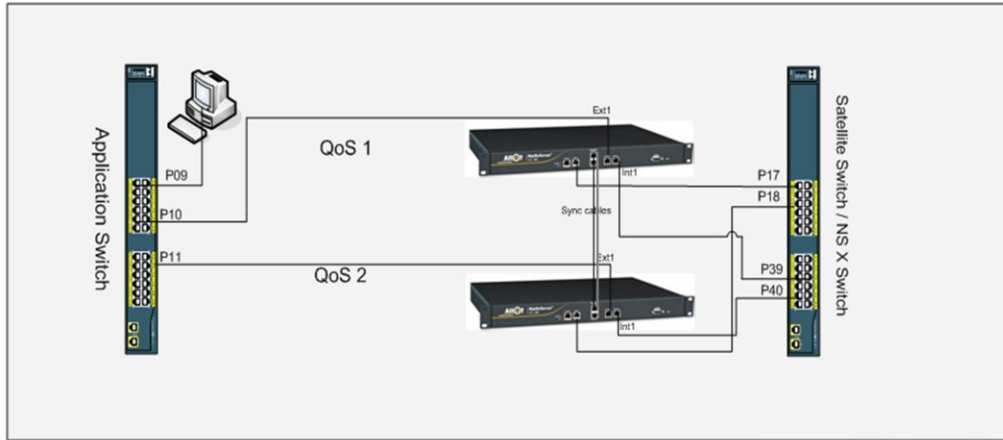
The Internal port of the NetEnforcer interfaces with the Hub (DPS) and the External port of the NetEnforcer interfaces with the border router.

The Bypass port is not in use.



NetEnforcer Active Redundancy

AC-502



Confidential and proprietary information

7

Both NetEnforcers are active, but only one is passing traffic.

If the primary link shuts down, the standby link starts forwarding traffic.

With bypass enabled, the secondary Enforcer will enter bypass state in case the both machines, primary and secondary are failed. In bypass mode the secondary machine will act as a wire – the traffic will pass, but no shaping will be enforced on it.

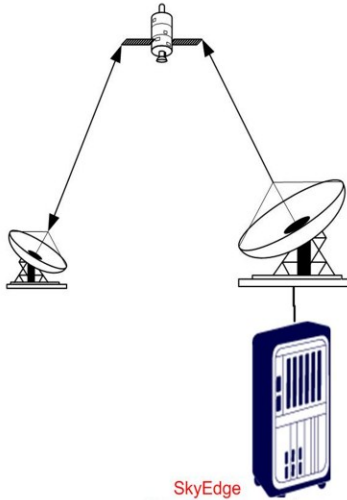
Both NetEnforcers share the same policy configuration.

Each NetEnforcer manages a single link while duplicating the link's traffic to the other NetEnforcer machine over the signaling ports.



Allot QoS System

Bandwidth configurations



- SEII OB = Allot IB
- Allot OB = SEII IB

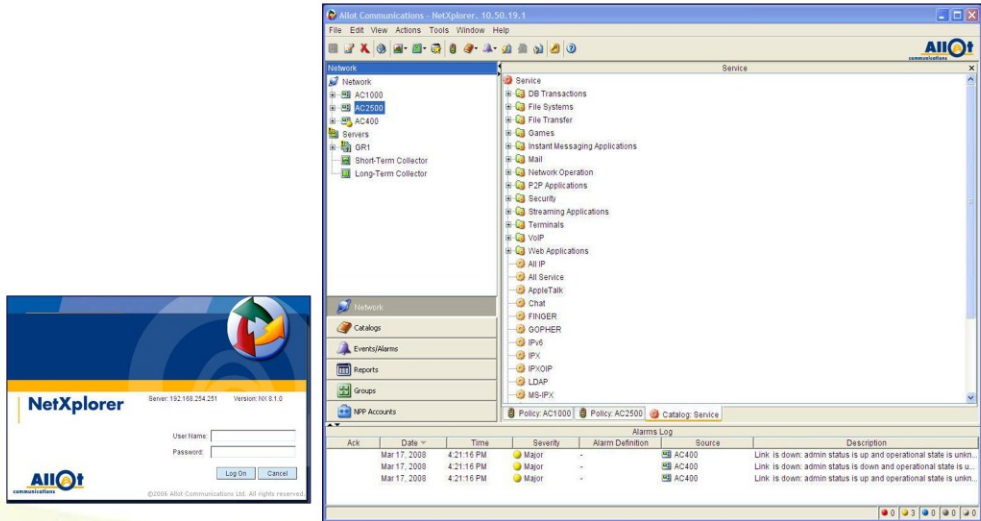
Confidential and proprietary information



Allot NetXplorer

NetXplorer GUI Client

- The NetXplorer Graphic User Interface Client
- It is needed to have Java 1.6 JRE (Java Run Environment) installed



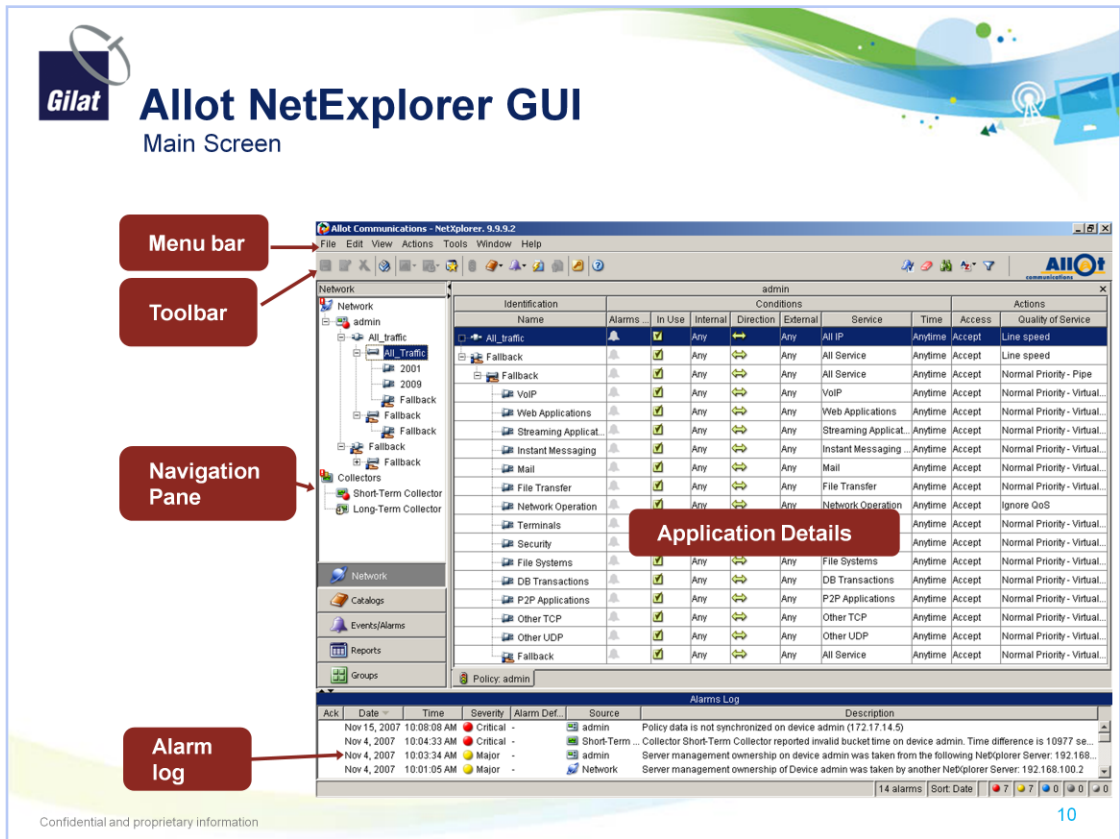
Confidential and proprietary information

To connect to the NetXplorer GUI:

1. In Internet Explorer of the Remote PC (SE) or Management PC (SEII), browse to <http://<<NetX IP>>> and select Launch NetXplorer in the NetXplorer Control Panel **OR** Double click the shortcut icon on the desktop or in the system's *Start menu*.
2. The Java Application Starting window is displayed.
3. The NetXplorer Log On dialog is displayed.

Enter User: Allot

Enter Password: \$SatCom\$ or 4SatCom4



Menu bar:

The NetXplorer menu bar provides easy access to the key functionality of the NetXplorer applications. Includes the File, Edit, View, Actions, Tools, Windows and Help menus.

Toolbar:

Shortcut buttons providing easy access to key NetXplorer functionality.

Navigation Pane:

The Navigation pane is divided into two sections. The lower portion of the Navigation pane enables you to select and open various NetXplorer applications. The upper portion of the pane displays a tree-like list of subcomponents or entries according to the application selected in the portion.

Details:

The Application Details pane displays data regarding the currently active applications and operations. A tab is displayed at the bottom of the pane for each open application. You can navigate easily between the open applications by clicking the tabs.

Alarm log:

The Alarms Log displays a list of the alarms triggered by the alarm definitions. The Alarms Log is automatically refreshed every 30 seconds. The severity of an alarm is indicated by the color of the icon (Info: light gray, Warning: dark gray; Minor: blue; Major: yellow; Critical: red). A checkmark in the leftmost column indicates that the alarm has been acknowledged. The status bar at the bottom of the Alarms Log indicates the total number of active alarms, and provides their breakdown according to severity.



QoS Policy Configuration

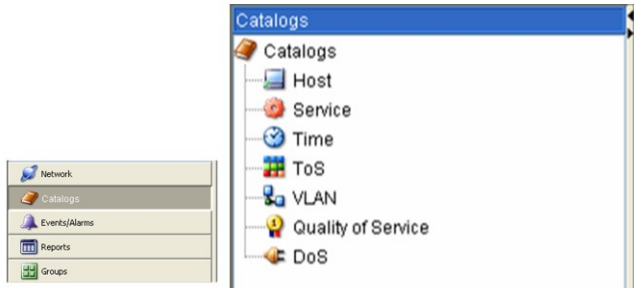




QoS Policy Configuration

Catalogs

- **Catalogs represent objects to be used to build a QoS policy**
 - A QoS policy is applied to Objects that were previously defined in the catalog, thereby defining the classifications and actions for the policy

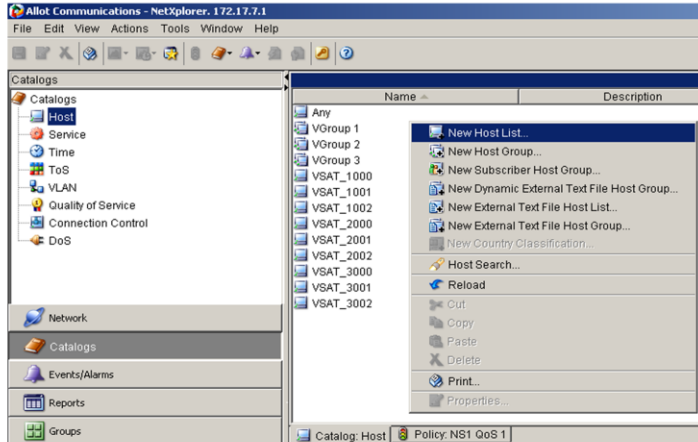
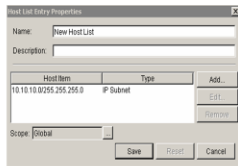
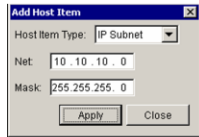




Host Catalog

Description

- A Host can be a network IP address, IP address range and IP subnet addresses.
 - Once you have defined the hosts in a host list, you can group several host lists together in one Catalog entry called Host Group



Confidential and proprietary information

Example of Hosts:

IP Address: The IP address of a host. For example, 172.16.1.31.

IP Subnet: For example, 10.10.10.0 with a subnet mask of 255.255.255.0.

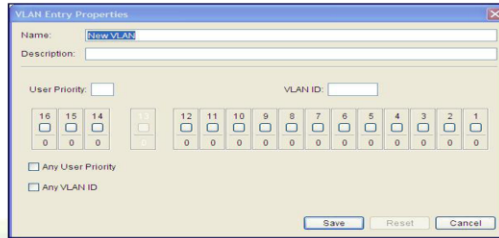
IP Range: A range of IP addresses. For example, 10.1.2.3-10.1.3.7 means the ranges 10.1.2.3-10.1.2.255 and 10.1.3.1-10.1.3.7.



VLAN Catalog

Description

- The VLAN Catalog contains Virtual LAN entities defined in the IEEE 802.1 Standard
- NetEnforcer supports VLAN traffic classification according to VLAN ID (VLAN Identifier) tags, consisting of 12 bits
- Insert bit values in one of the following ways
 - Insert a decimal value in the VLAN ID fields
 - The binary equivalent is displayed in the bit value fields
 - Click the bit value field boxes (zero is indicated as gray and black as one)
 - The decimal equivalent is displayed in the User Priority and VLAN ID fields



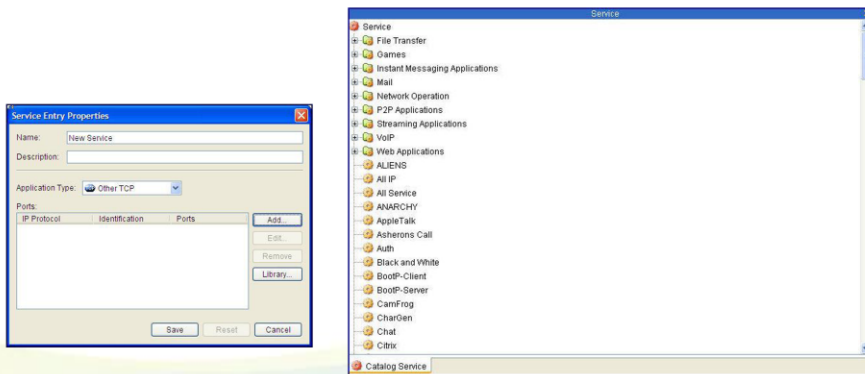
Confidential and proprietary information



Service Catalog

Description

- The Service defines the applications, protocol specifications (including network protocols, transport protocols and application protocols) of the connection passing through a NetEnforcer
- The Service Catalog contains two types of objects
 - Services - Specific Application or Protocol
 - Service Groups - Multiple Services Group



Confidential and proprietary information

Services are the protocol or application-based criteria for traffic classification. A service can exist in only one location in the hierarchy at any given time. Depending on the type of service, specific content entries can be defined in order to enable the policy assignment and monitoring at the content level.

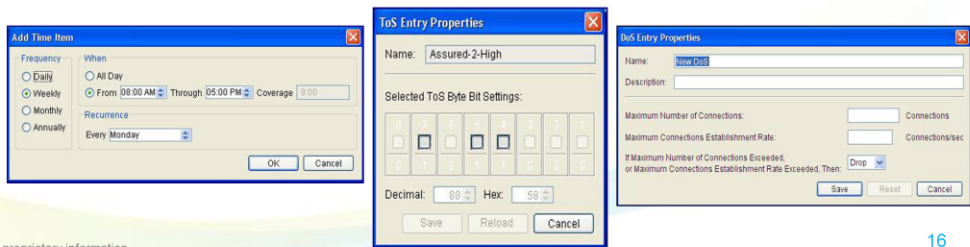
Service Groups enable you to efficiently assign policies to multiple services, instead of having to define separate policies on a service-by-service basis. Service groups also enable you to generate reports for specific groups of services.



Time, ToS and DoS Catalogs

Description

- **The Time Catalog contains entries that are the possible values for the time condition**
 - The Anytime entry is Protected, meaning the definitions for this entry cannot be modified
- **The ToS Catalog contains entries that are the possible values for the ToS (Type of Service) condition**
 - All of the ToS byte markings are predefined in the ToS Catalog
- **The DoS (Denial of Service) Catalog enables you to control the number of connections and the rate of connections established per policy**



Time periods in the Time Catalog can have ranges of hours and minutes in which they are active, or they can be active during whole days. An entry in the Time Catalog has one or several time periods when policies assigned this entry are active.

The ToS is a byte in the IP header of a packet that contains information about routing recommendations. NetEnforcer classifies traffic based on the ToS byte marking contained in the IP headers of the packets passing through it.

In the DoS Catalog Each entry indicates the maximum number of connections that can be established, the maximum rate of connections established and what action should be taken if the maximum establishment exceeded or when the maximum of connections exceeded.

Gilat **QoS Catalog**
Description

- The QoS Catalog contains entries that are the possible values for the Quality of Service action
- It is necessary to define QoS policies valid for each one of the hierarchy levels separately
 - There are different QoS Policies for
 - Line Enhanced QoS
 - Pipe Enhanced QoS
 - VC Enhanced QoS
 - In the Enhanced QoS Catalogs we can define
 - CIR and MIR
 - Minimum Reserved on USE (Pipe only)
 - Priority Levels (1 to 4 + Best Effort)
 - EF (VC only)
 - Drop Precedence (VC only)

Confidential and proprietary information

17

In NetEnforcer machines of version AC-501 we use the Enhanced QoS catalogs.

The Ignore QoS, Line speed, Normal Priority – Pipe and Normal Priority - Virtual Channel entries are protected, meaning the definitions for these entries cannot be modified.

The QoS Catalog enables you to define QoS for a Line, Pipe or Virtual Channel. We can prioritize connections and specify minimum and maximum bandwidth per Line/Pipe/Virtual Channel, and we can specify Drop Precedence for Virtual Channels.

It is possible to configure the action to be taken if minimum bandwidth is not allocated, by selecting one of the following options from the designated dropdown list:

Admit by Priority: Accept the new connection, but do not assign the minimum bandwidth. The new connection gets bandwidth per priority.

Bypass: The traffic will pass through the system, but without any QoS.

Drop: All packets are dropped. The user is disconnected and may see the message *Connection timed-out*.





QoS Principles

Expedited Forwarding (RFC 2598)

- Intended for real time applications sensitive to loss, delay and jitter
- No buffering is used to minimize jitter and delay
- Traffic that can't be allocated will be dropped



Confidential and proprietary information

18

Expedited forwarding enables first-class service level for real time traffic which is loss-sensitive, delay-sensitive and jitter-sensitive and can also handle traffic bursts efficiently. With this feature users can ensure QoE for real-time applications such as VoIP and Videoconferencing services. Allot's implementation of this feature is in accordance with RFC2598.

Expedited forwarding traffic (unlike traffic for which a regular "maximum" is defined) is not smoothed. Unlike traffic for which a regular maximum is defined, the Expedited forwarding defined rate can be allocated entirely in the first millisecond (burst). When starting to transmit in the middle of the second the traffic is allowed to breach the maximum of the hierarchy object above. In order to provide the specified rate to be Expedited, the QoS engine provides this rate at the expense of other VC's in the subsequent second.

6



QoS Principles

Expedited Forwarding (RFC 2598)

- **Definitions**

- BW defined in kbps
- Minimum = Maximum
- Available only from Enhanced VC QoS catalog

Virtual Channel Enhanced QoS Entry Properties

Name:

Description:

Virtual Channel Based QoS Coverage:

Inbound and Outbound

Expedited Forwarding Bandwidth:

Expedited Forwarding

Drop Precedence:

If Minimum Virtual Channel Bandwidth not Allocated:



QoS Principles

Assured Forwarding (RFC 2597)

- **Assured Forwarding (AF) standard offers 4 different levels of forwarding assurances as long as the traffic does not exceed the Max rate**
- **When the traffic exceeds the max rate, the packets will be buffered or dropped according to the “Drop Precedence”**

	Class 1	Class 2	Class 3	Class 4
Low Drop Precedence	Low1	Low2	Low3	Low4
Medium Drop Precedence	Med1	Med2	Med3	Med4
High Drop Precedence	Hi1	Hi2	Hi3	Hi4

- **Priority - 4 standard classes supported (all policy levels)**
- **Drop Precedence – 3 standard levels supported (VC only)**

Confidential and proprietary information

20

Allot’s enhanced QoS engine provides support for RFC 2597 (Assured Forwarding) by offering 4 levels of priority (as opposed to 10 in the legacy QoS) and 3 levels of drop precedence (supported at the VC level only). When viewed together, this gives us the 12 levels of service stipulated in the assured forwarding RFC.

When traffic exceeds the maximum rate set, the decision on whether to buffer or drop packets will be taken according to the drop precedence value assigned to each packet. Packets with a high drop precedence will be dropped before packets with a low drop precedence.



QoS Principles

Assured Forwarding (RFC 2597)

- If a packet is not transmitted to the network, it will be dropped or buffered
- Drop precedence value determines the importance of the packet before making the decision to buffer or not
- Packets with higher drop precedence values are discarded before packets with lower drop precedence

Virtual Channel Enhanced QoS Entry Properties

Name:

Description:

Virtual Channel Based QoS Coverage:

Inbound and Outbound

Minimum Bandwidth (Kbps):

Maximum Bandwidth (Kbps): Maximum Allowed

Priority (Best Effort)

Priority (1 Lowest, 4 Highest)

Expedited Forwarding

Drop Precedence: **No Buffering**
Low
Medium
High
Application Based

If Minimum Virtual Channel Bandwidth

Confidential and proprietary information

21

The default drop precedence value is “Application Based”, whereby high, medium and low values are pre-defined in the software code per application type.



QoS Principles

Best Effort

- Available for Line, Pipe and VC QoS catalogs
- If all objects in the same policy level are set to “Best Effort”, there will be no prioritization between objects, i.e. the bandwidth will be divided proportionally to ingress
- If some traffic on the same policy level is prioritized (1-4) and other set to “Best Effort”, in scenario of congestion, the “Best Effort” traffic will get no resources
- “Best Effort” is defined by default. Gilat recommends to change it to any priority (1-4), in order to prevent potential starvation

Pipe Enhanced QoS Entry Properties

Name:

Description:

Pipe Based QoS Coverage:

Inbound and Outbound

Minimum Bandwidth (Kbps):

Maximum Bandwidth (Kbps): Maximum Allowed

Minimum Bandwidth Reserved on Use

Priority (Best Effort)

Priority (1 Lowest, 4 Highest)

If Minimum Pipe Bandwidth not Allocated:

Confidential and proprietary information



QoS Principles

Working with Priorities

- A priority definition implies a relative bandwidth allocation relative to other defined priorities
- A priority does not indicate absolute bandwidth allocations
- Bandwidth is allocated to each element by dividing the element weight (1,2,3 or 4) by the total weight of all the entities in competition with each other, (e.g: 1+4) and multiplying by the total available bandwidth (e.g: the maximum bandwidth defined).



$$\text{Allocated Bandwidth} = \text{Minimum} + \frac{\text{Element Weight}}{\text{Total Weight}} \times \text{Total Bandwidth Available}$$

Confidential and proprietary information

23

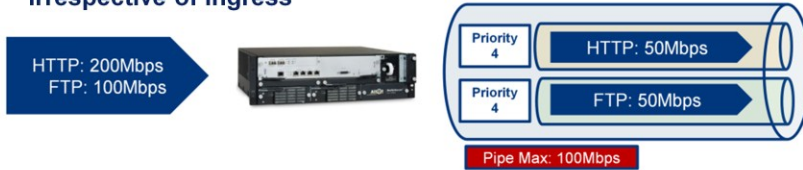
The allocation of bandwidth is done irrespective of the ingress rates.



QoS Principles

Equal Priority vs Best Effort

- If Equal Priorities are set, the bandwidth is assigned equally and irrespective of ingress



- If Best Effort is set, the bandwidth is allocated proportionately to ingress



$$\text{Allocated Bandwidth} = \frac{\text{Ingress Application Traffic}}{\text{Total Ingress traffic}} \times \text{Total Bandwidth Available}$$

Confidential and proprietary information



QoS Principles

Minimum + Equal Priority

- If Minimum + Equal Priorities are set, the minimum first assigned to each element
- Remaining bandwidth then assigned according to priority weighting and regardless to ingress



Remaining Bandwidth after min. allocation = Total Bandwidth Available – (Total Minimum)

Remaining Bandwidth after min. allocation = 200 – (80 + 20) = 100 Mbps

Allocated Bandwidth = Minimum + $\frac{\text{Element Weight}}{\text{Total Weight}} \times \text{Remaining Bandwidth}$

Allocated Bandwidth for HTTP = 80 + 4 / 8 X 100 = 130 Mbps

Allocated Bandwidth for FTP = 20 + 4 / 8 X 100 = 70 Mbps

Confidential and proprietary information

25



QoS Principles

Minimum + Best Effort

- If Minimum + Best Effort are set, the minimum first assigned to each element
- The remaining bandwidth will be divided in such manner that will complete to the values proportional to the ingress



Confidential and proprietary information

26

If the NetXplorer operator assigns each VC with the default “best effort” priority alongside the minimum, then as long as the maximum bandwidth is larger than the total of guaranteed bandwidth, bandwidth will be divided in proportion to the ingress traffic – in this case, both VC’s will be assigned 100Mbps. If there was no minimum defined, the expected total Bandwidth for each pipe would be $[200/(200+200)]*200M=100Mbps$. If the minimum guaranteed for each VC is less than the expected value, then the output will be the same as if there was no minimum.



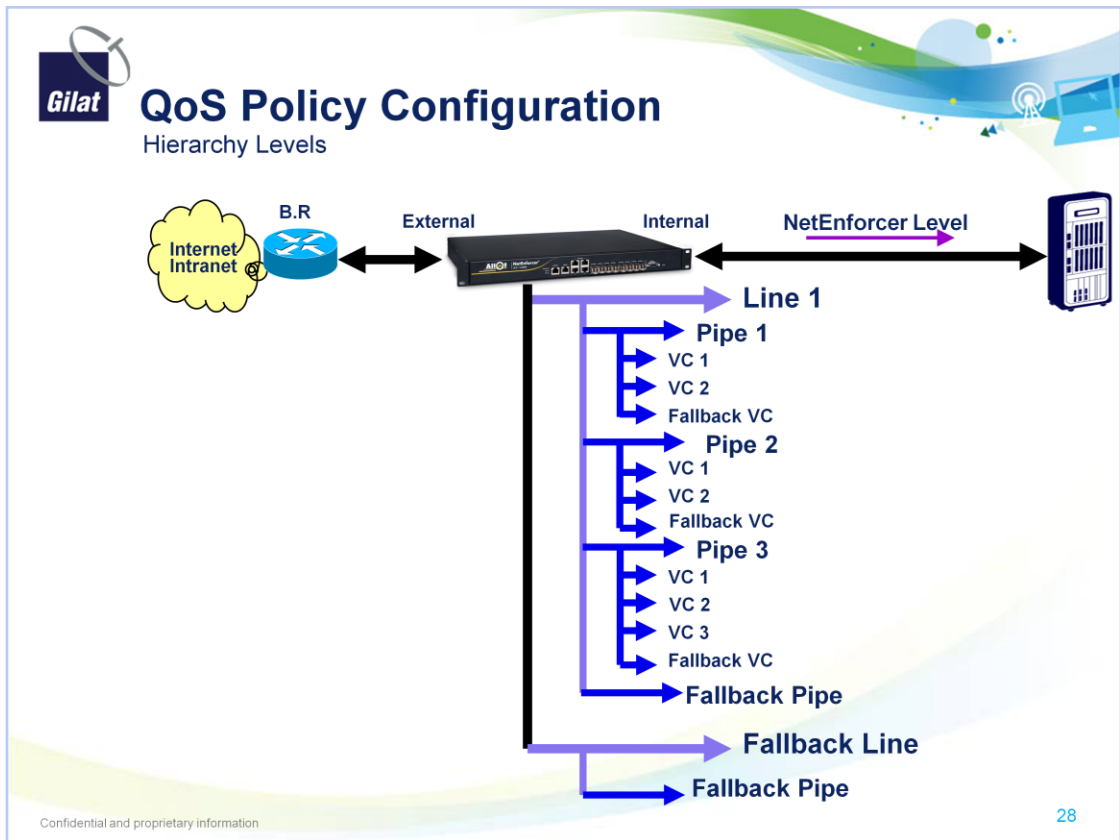
QoS Policy Configuration

Hierarchy levels

- QoS policy consists of a set of “Conditions” and a set of “Actions” that apply as a consequence of the conditions being satisfied
- Traffic is classified using Lines, Pipes and Virtual Channels
 - A Line, Pipe or Virtual Channel is defined by one or more Conditions and a set of actions
 - A Line includes one or more Pipes
 - A Pipe includes one or more Virtual Channels
- Classification Level Hierarchy
 1. NetEnforcer
 2. Line
 3. PIPE
 4. VC (Virtual Channel)

NE-Central											
Name	Alarms	In Use	Conditions						Actions		
			Internal	Direct.	External	Service	Time	ToS	VLAN	Access	Quality
Fallback		<input checked="" type="checkbox"/>	Any	↕	Any	All Service	Anytime	Any	Any	Accept	Line sp...
P2P Applications		<input checked="" type="checkbox"/>	Any	↕	Any	P2P App.	Anytime	Any	Any	Accept	Normal...
Voice		<input checked="" type="checkbox"/>	Any	↕	Any	VoIP	Anytime	Any	Any	Accept	Normal...
Web Applications		<input checked="" type="checkbox"/>	Any	↕	Any	Web App.	Anytime	Any	Any	Accept	Normal...
Streaming Applications		<input checked="" type="checkbox"/>	Any	↕	Any	Streams...	Anytime	Any	Any	Accept	Normal...
Instant Messaging		<input checked="" type="checkbox"/>	Any	↕	Any	Instant M.	Anytime	Any	Any	Accept	Normal...
Mail		<input checked="" type="checkbox"/>	Any	↕	Any	Mail	Anytime	Any	Any	Accept	Normal...
File Transfer		<input checked="" type="checkbox"/>	Any	↕	Any	File Tran.	Anytime	Any	Any	Accept	Normal...
Network Operation		<input checked="" type="checkbox"/>	Any	↕	Any	Network	Anytime	Any	Any	Accept	Normal...
Fallback		<input checked="" type="checkbox"/>	Any	↕	Any	All Service	Anytime	Any	Any	Accept	Normal...

Confidential and proprietary information



When you add a new Pipe, it always includes at least one Virtual Channel, the Fallback Virtual Channel. The Condition of the Fallback Virtual Channel cannot be modified or deleted.

Fallback of any level can not be deleted.

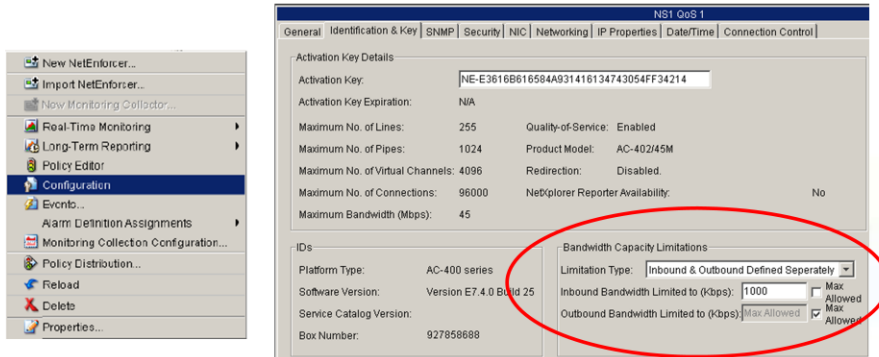
The action for Fallback of any level can be modified.



Hierarchy Level

NetEnforcer Level

- The NetEnforcer Levels represents the Outbound capacity
 - For SE set the "Inbound Bandwidth Limited to" 95% of SE Outbound bit rate (Kbps)
 - For SEII ACM, Outbound is defined automatically by the hub DPS



Confidential and proprietary information

In SkyEdge the NetEnforcer Level is assigned to approximately 95% of the HUB MIR.
 In SkyEdge II the NetEnforcer Level is automatically assigned by the designated DPS.

When using SE in the Outbound, uncheck the (Allot Inbound) Max Allowed checkbox and set Inbound Bandwidth Limited to (Kbps) to 95% of SE Outbound bandwidth. When using SEII ACM, Outbound is defined automatically by the hub DPS. Select (check) the (Allot Outbound) Max Allowed checkbox.



QoS Policy Configuration

Example

- Conditions can be defined at Line level, Pipe level or VC level.

Internal Hosts – VSATs

Service – Application

Other Conditions

Name	Alarms ...	In Use	Conditions							Actions	
			Internal	Directi...	External	Service	Time	ToS	VLAN	Access	Quality ...
Fallback		<input checked="" type="checkbox"/>	Any	↔	Any	All Service	Anytime	Any	Any	Accept	Line sp...
Fallback		<input checked="" type="checkbox"/>	Any	↔	Any	All Service	Anytime	Any	Any	Accept	Normal ...
P2P Applications		<input checked="" type="checkbox"/>	Any	↔	Any	P2P App...	Anytime	Any	Any	Accept	Normal ...
VoIP		<input checked="" type="checkbox"/>	Any	↔	Any	VoIP	Anytime	Any	Any	Accept	Normal ...
Web Applications		<input checked="" type="checkbox"/>	Any	↔	Any	Web App...	Anytime	Any	Any	Accept	Normal ...
Streaming Applications		<input checked="" type="checkbox"/>	Any	↔	Any	Streami...	Anytime	Any	Any	Accept	Normal ...
Instant Messaging		<input checked="" type="checkbox"/>	Any	↔	Any	Instant M...	Anytime	Any	Any	Accept	Normal ...
Mail		<input checked="" type="checkbox"/>	Any	↔	Any	Mail	Anytime	Any	Any	Accept	Normal ...
File Transfer		<input checked="" type="checkbox"/>	Any	↔	Any	File Tran...	Anytime	Any	Any	Accept	Normal ...
Network Operation		<input checked="" type="checkbox"/>	Any	↔	Any	Network ...	Anytime	Any	Any	Accept	Normal ...
Fallback		<input checked="" type="checkbox"/>	Any	↔	Any	All Service	Anytime	Any	Any	Accept	Normal ...

Policy NE-Central

Confidential and proprietary information



QoS Policy Configuration

Example

- **Actions will be enforced for a condition that is met**
 - A specific connection can be accepted or blocked
 - If it is accepted, a QoS catalog is enforced for this connection

NE-Central											
Name	Alarms ...	In Use	Internal	Directi...	Conditions					Actions	
					External	Service	Time	ToS	VLAN	Access	Quality
[-] Fallback		<input checked="" type="checkbox"/>	Any	↔	Any	All Service	Anytime	Any	Any	Accept	Line sp...
[-] Fallback		<input checked="" type="checkbox"/>	Any	↔	Any	All Service	Anytime	Any	Any	Accept	Normal ...
[-] P2P Applications		<input checked="" type="checkbox"/>	Any	↔	Any	P2P App...	Anytime	Any	Any	Accept	Normal ...
[-] VoIP		<input checked="" type="checkbox"/>	Any	↔	Any	VoIP	Anytime	Any	Any	Accept	Normal ...
[-] Web Applications		<input checked="" type="checkbox"/>	Any	↔	Any	Web App...	Anytime	Any	Any	Accept	Normal ...
[-] Streaming Applications		<input checked="" type="checkbox"/>	Any	↔	Any	Streami...	Anytime	Any	Any	Accept	Normal ...
[-] Instant Messaging		<input checked="" type="checkbox"/>	Any	↔	Any	Instant M...	Anytime	Any	Any	Accept	Normal ...
[-] Mail		<input checked="" type="checkbox"/>	Any	↔	Any	Mail	Anytime	Any	Any	Accept	Normal ...
[-] File Transfer		<input checked="" type="checkbox"/>	Any	↔	Any	File Tran...	Anytime	Any	Any	Accept	Normal ...
[-] Network Operation		<input checked="" type="checkbox"/>	Any	↔	Any	Network ...	Anytime	Any	Any	Accept	Normal ...
[-] Fallback		<input checked="" type="checkbox"/>	Any	↔	Any	All Service	Anytime	Any	Any	Accept	Normal ...

Confidential and proprietary information



QoS Policy Configuration

Using Templates

- **Templates enable you to create a "master" Pipe or VC that will create duplicate Pipes or VCs for each connection**
- **In SE and SEII we use templates on pipe level**
- **When using a pipe template**
 - **Each Host in the Host Group of the pipe will get the Pipe rule separately**
- **When using a regular Pipe**
 - **All hosts in the Host group of the pipe, will share the pipe rule**

Confidential and proprietary information

32

The concept of using Template is to eliminate the need to define individual Pipes if the only difference is the source or destination IP address.

Pipe templates enable you to automatically add instances of the same Pipe for each host in a selected Host Catalog entry.

If assigning a Host (not a Host Group) to a Pipe template, each IP in the range will get the pipe rule.



QoS Policy Configuration

Using Distribution

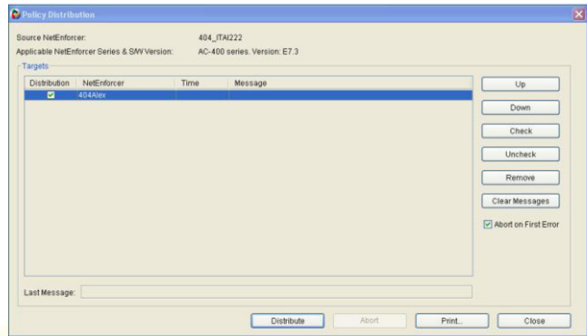
- Using the Policy Distribution feature it is possible to update the policies of one unit and then distribute the new policies to other NetEnforcer units on the Network
- All NetEnforcers must be of the same Series and running the same major software version

To distribute Policies:

In the Navigation pane, right-click a NetEnforcer in the Navigation tree and select Policy Distribution from the popup menu.

OR

Select a NetEnforcer in the Navigation tree and then select Policy Distribution from the View menu.



Confidential and proprietary information



Gilat Recommended Configuration





QoS Policy Configuration

Gilat Recommendation – VLAN 24

- **NetEnforcer Level – Outbound Rate**
 - All traffic passing through the device
- **LINE Level - MPN #**
 - No classification is defined
 - The classification is determined by the Pipe policies defined under it
- **PIPE Level - VSAT IP Subnet**
 - Pipe Template policy, classification specified by IP Subnets using a Host Group. The Host Group catalog object represents the VSATs that have the same SLA
 - The policy is assigned with a QoS object
- **VC - Applications**
 - Classification specified by Applications/Protocols
 - The policy is assigned with a QoS object

Confidential and proprietary information

35

In a SkyEdge II network with ACM, the NetEnforcer level can change dynamically.



QoS Policy Configuration

Example of Configuration – VLAN 24

- **The Line Level**
 - Pipes related to MPN #1
 - No Classification and no Action are configured at this Level.
- **The Pipe level (SLA per Group of VSAT IP Subnet) as follows:**
 - **Pipe #1(Platinum)**
 - Classification Object - Host Group - VSAT IP Subnet
 - QoS Object – MIR 750 Kbps
 - **Pipe #2 (Gold)**
 - Classification Object - Host Group - VSAT IP Subnet
 - QoS Object – MIR 500 Kbps
 - **Pipe #3(Silver)**
 - Classification Object - Host Group - VSAT IP Subnet
 - QoS Object – MIR 250 Kbps

Confidential and proprietary information

36

In VSAT (IP Subnet) template case:

In a situation that VSAT serves a single network behind network.

This level's classification is specified by the IP subnets that belong to a Host Group. The Host Group catalog Object represents VSATs with the same SLA.

The Pipe policy is applied to a QoS object.



QoS Policy Configuration

Example of Configuration – VLAN 24

- **Virtual Circuit (VC) Applications**
 - **VC #1**
 - QoS Object for VoIP - priority 4
 - **VC #2**
 - QoS Object for TCP port 12345 - priority 3
 - **VC #3**
 - QoS Object for HTTP - priority 2
 - **VC #4**
 - QoS Object for FTP - priority 1



Thank You



Boundless Communications
