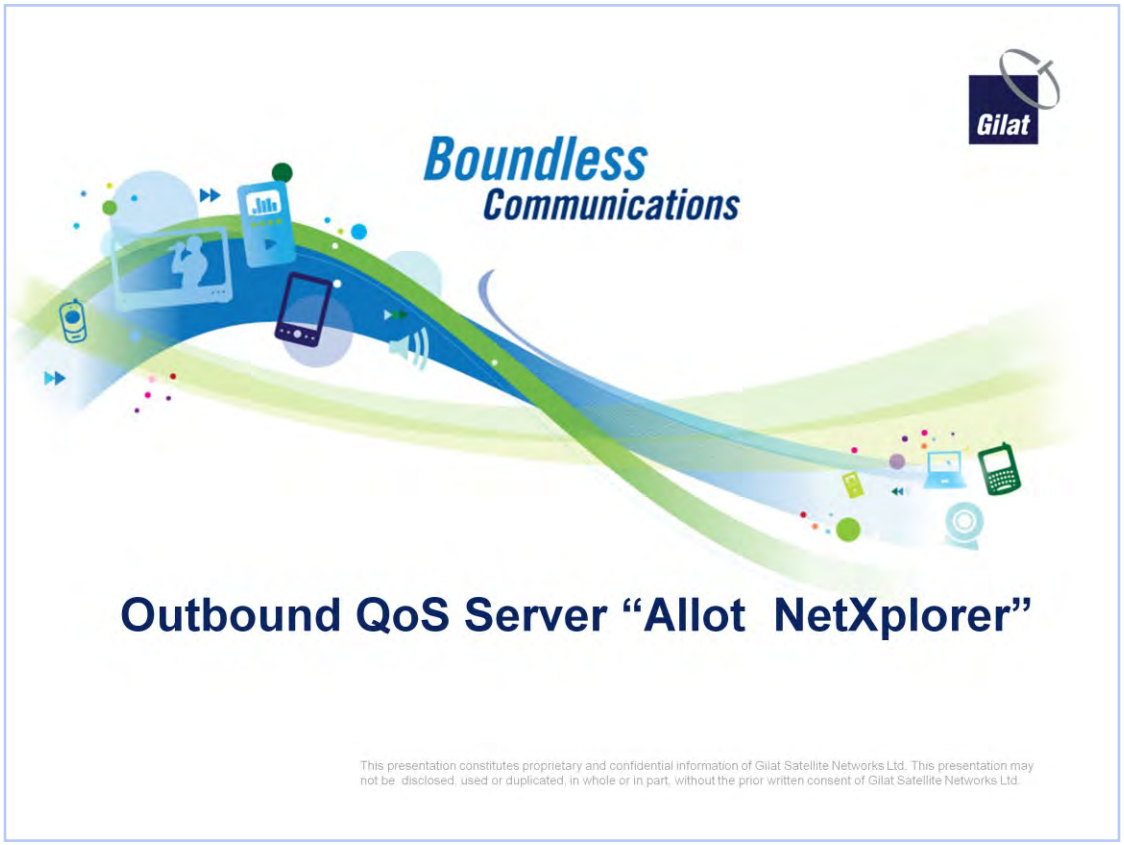
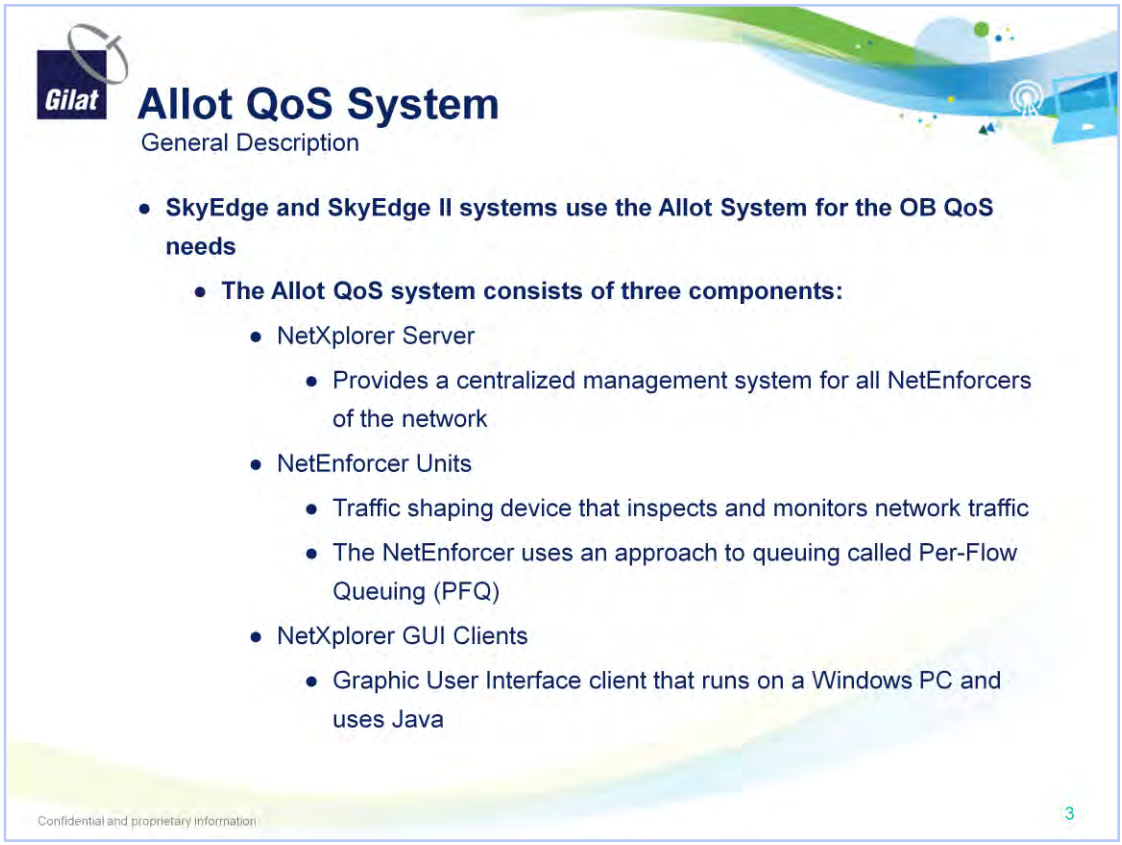



Gilat
Session Objectives
General Description
NetXplorer Server
Monitoring
NetEnforcer
Hardware Description
Active Redundancy
Bypass Mode
Connectivity
NetXplorer GUI Client
QoS Policy Configuration
Catalogs
Hierarchy Levels
Conditions
Actions
Recommended Gilat Configuration
allot communications
Confidential and proprietary information
2

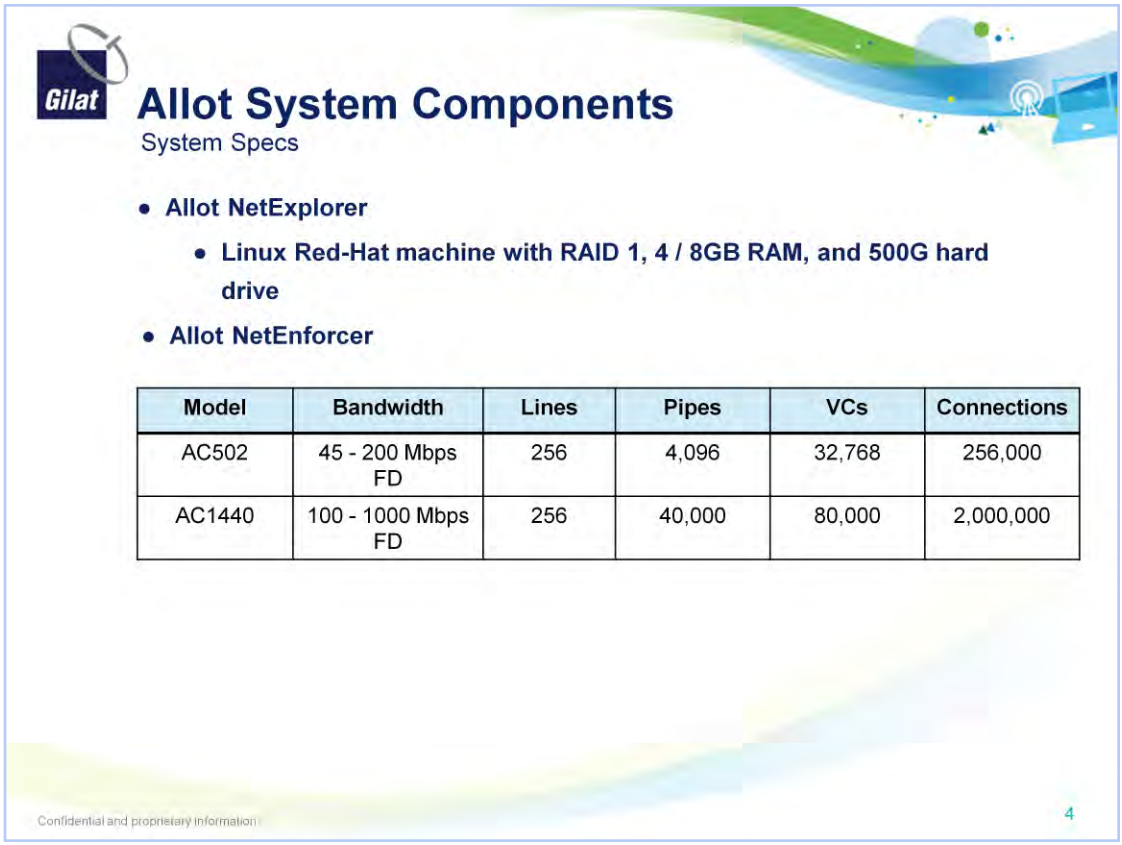


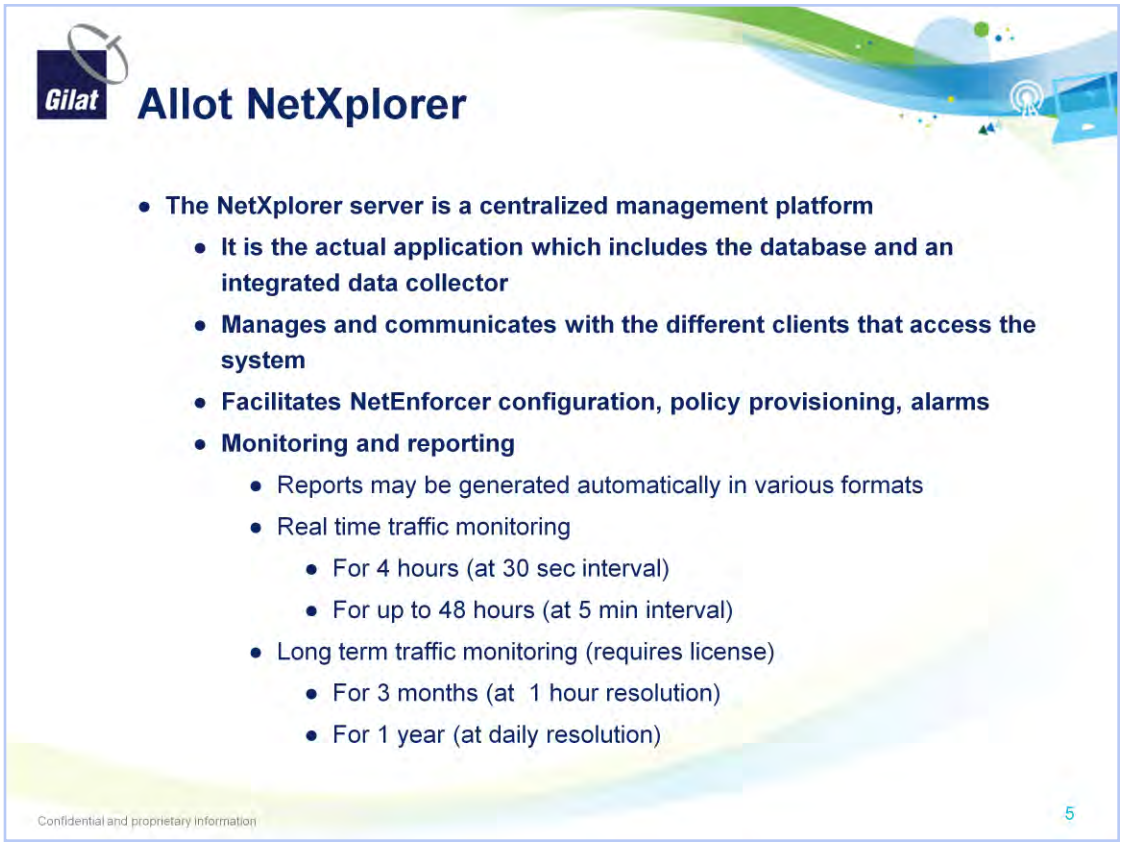
Allot's Per-Flow Queuing

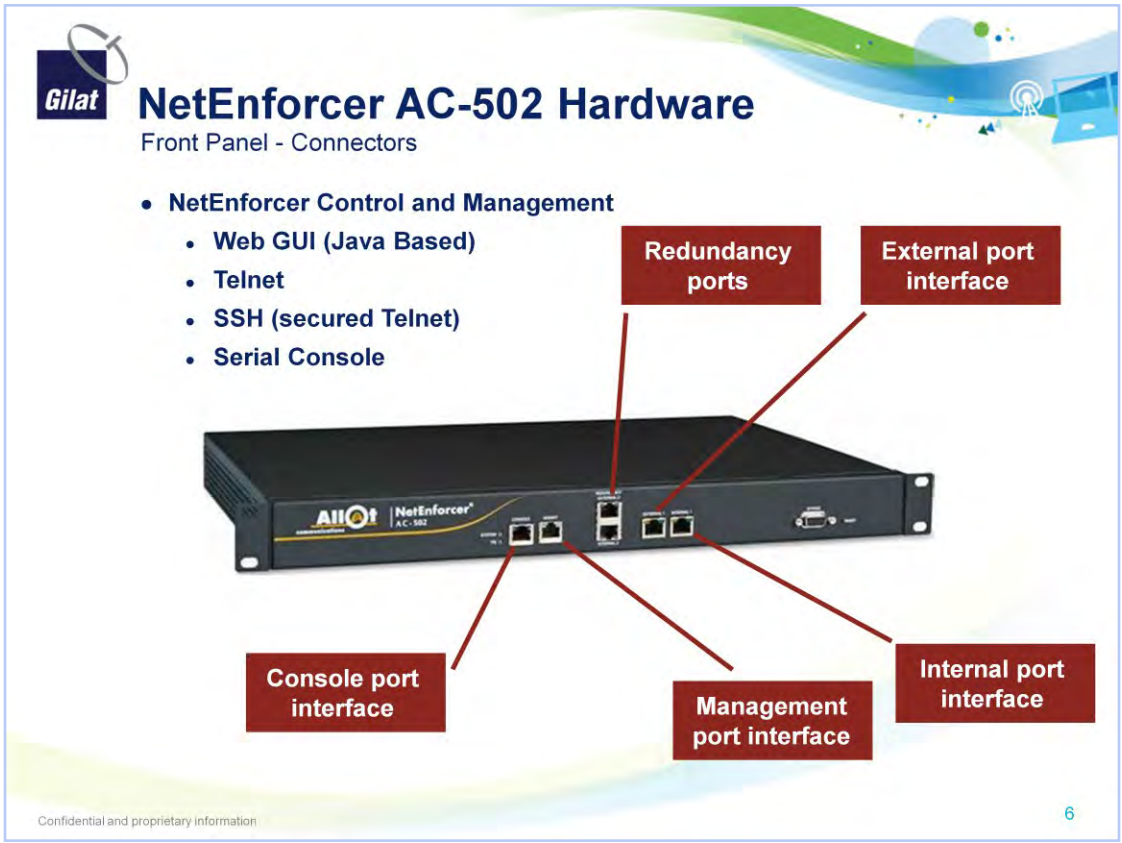
The NetEnforcer uses an approach to queuing called Per-Flow Queuing (PFQ). Each flow gets its own queue and is treated individually. This enables the NetEnforcer to offer very accurate traffic shaping. Per-flow Queuing uses TCP's inherent flow control to achieve the maximum and most efficient bandwidth usage. Per-Flow Queuing exploits two important internal mechanisms of TCP, the "Slow Start" and "Congestion Avoidance"'. These mechanisms gradually increase the rate of the data flow until they identify that the link between the two end points is saturated. PFQ takes advantage of these mechanisms by artificially and dynamically enforcing the proper transmitting rate per flow in a way that will meet the policy requirement and will avoid collisions. The transmitting TCP will then synchronize to the rate dictated by the NetEnforcer. The NetEnforcer thus "forces" each flow to transmit packets in the rate that will meet the user defined Policy, including the minimum, maximum and priority definitions.

How It Works

Allot's Per-Flow Queuing is implemented by the QoS Enforcement Module in the NetEnforcer. Each packet that arrives into the NetEnforcer is matched to the proper flow by the Flow Identifier, and inserted to the queue of the proper flow. If the packet does not match any of the existing flows, the New Flow Generator examines the conditions of the flow and matches it to the proper policy. The new flow's queue is then added to the system. When the packet arrives to the QoS Enforcement Module, it checks whether the guaranteed bandwidth was exhausted and whether the maximum limitation was achieved. If the guaranteed bandwidth was not exhausted, the packet is transmitted immediately (without any delay). If the maximum limit for that flow has been reached, the packet is placed in a buffer. Otherwise the packet will be placed in its flow queue and will be transmitted based on the priority of the flow and the available bandwidth. The queues are generated and increased dynamically. A queue is generated per-flow and closed once the flow ends. This way the resources of the system are optimally used. The NetEnforcer manages a large buffer bank and dynamically assigns to each queue only the buffer size required for the flow at any given time. Thus even large temporary queues for certain peaks or bursts of a flow can be accommodated.


Gilat
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
AC1440 | 100 - 1000 Mbps FD | 256 | 40,000 | 80,000 | 2,000,000
Confidential and proprietary information
4

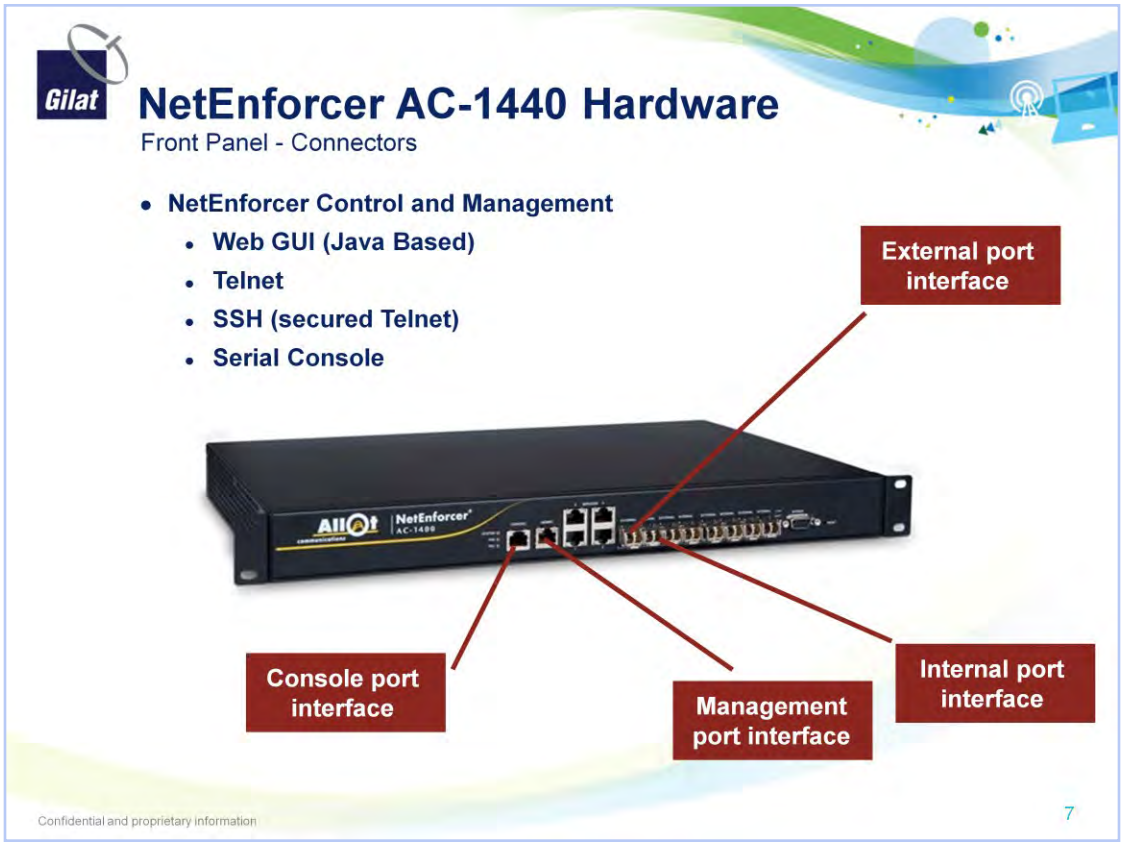

Gilat
Allot NetXplorer
The NetXplorer server is a centralized management platform
It is the actual application which includes the database and an integrated data collector
Manages and communicates with the different clients that access the system
Facilitates NetEnforcer configuration, policy provisioning, 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



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.

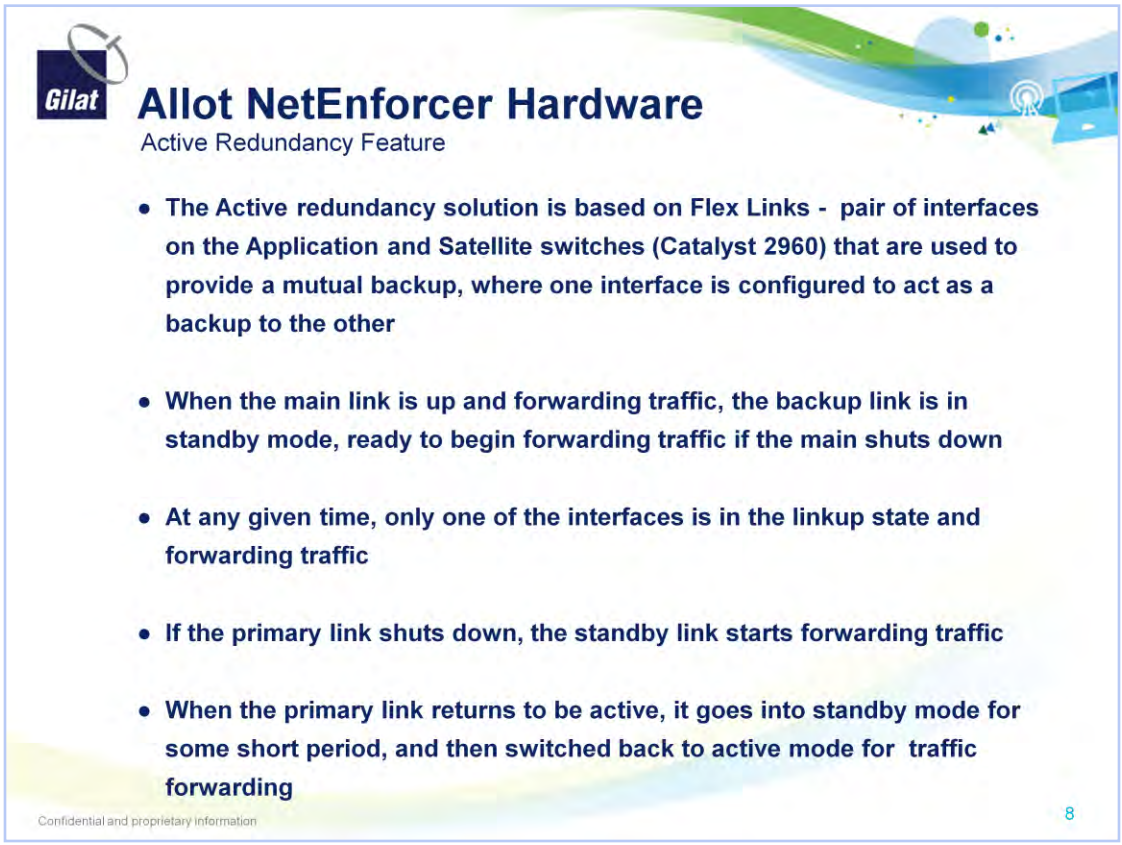
The Bypass port is not in use.



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.

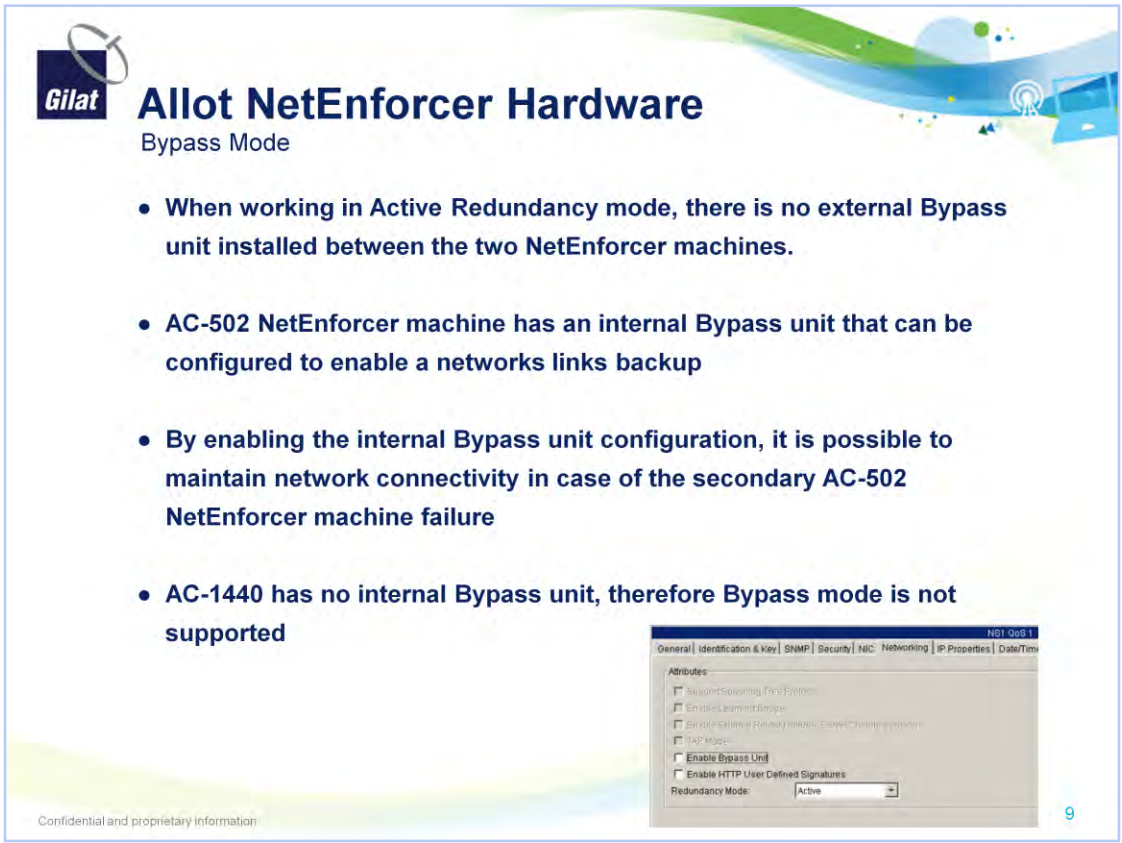
The Service and Bypass ports are not in use.



Operation

Operation of the Allot NetEnforcer machine (AC-1400 and AC-502) is based on the Active Redundancy concept. Both NetEnforcer machines are identified as active, share the same policy configuration, and receive Outbound transmission from the hub. At any point of time, only one of the NetEnforcer machines (**NS1 QoS 1**) is passing traffic. The two NetEnforcer machines communicate with each other using the Flex Links mechanism to determine which one of the NetEnforcer machines is passing traffic.

Active Redundancy is available only in Allot OS version 11.1.1 and higher.



Operation

AC-502

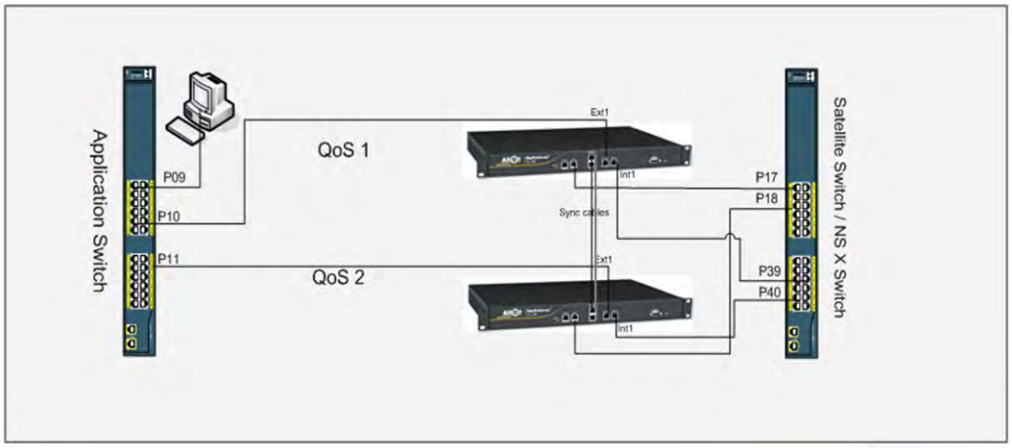
The internal Bypass unit must be enabled on secondary machine during the installation in order to enable bypass mode. With bypass enabled, the secondary Enforcer will enter bypass state in case the both machines, primary and secondary are failed. In bypass mode the secondary machine will act as a wire – the traffic will pass, but no shaping will be enforced on it.

AC-1440

There is no internal bypass unit. The bypass mode is optional only by installing external bypass machine, but it can't coexist together with active redundancy configuration. Therefore the bypass mode is not supported in AC-1440.

NetEnforcer Active Redundancy

AC-502



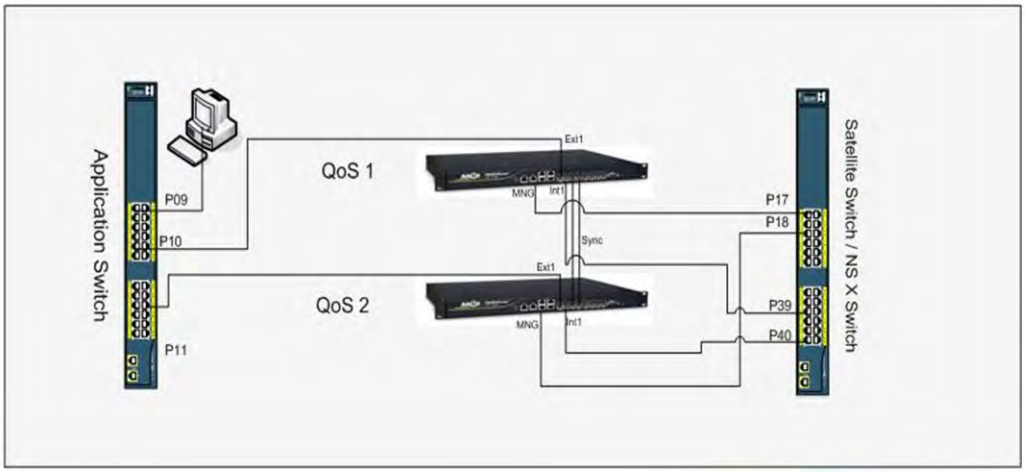
Both NetEnforcers are active, but only one is passing traffic.

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.

NetEnforcer Active Redundancy

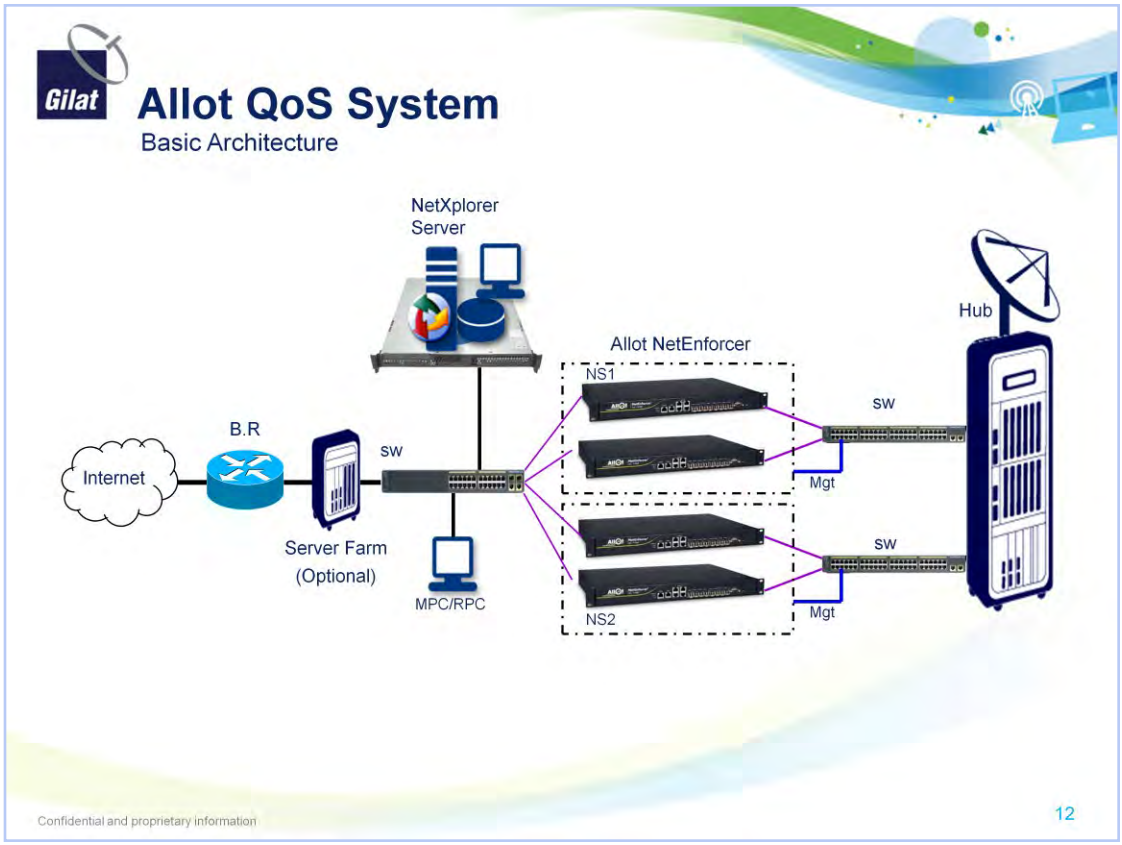
AC-1440



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

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.



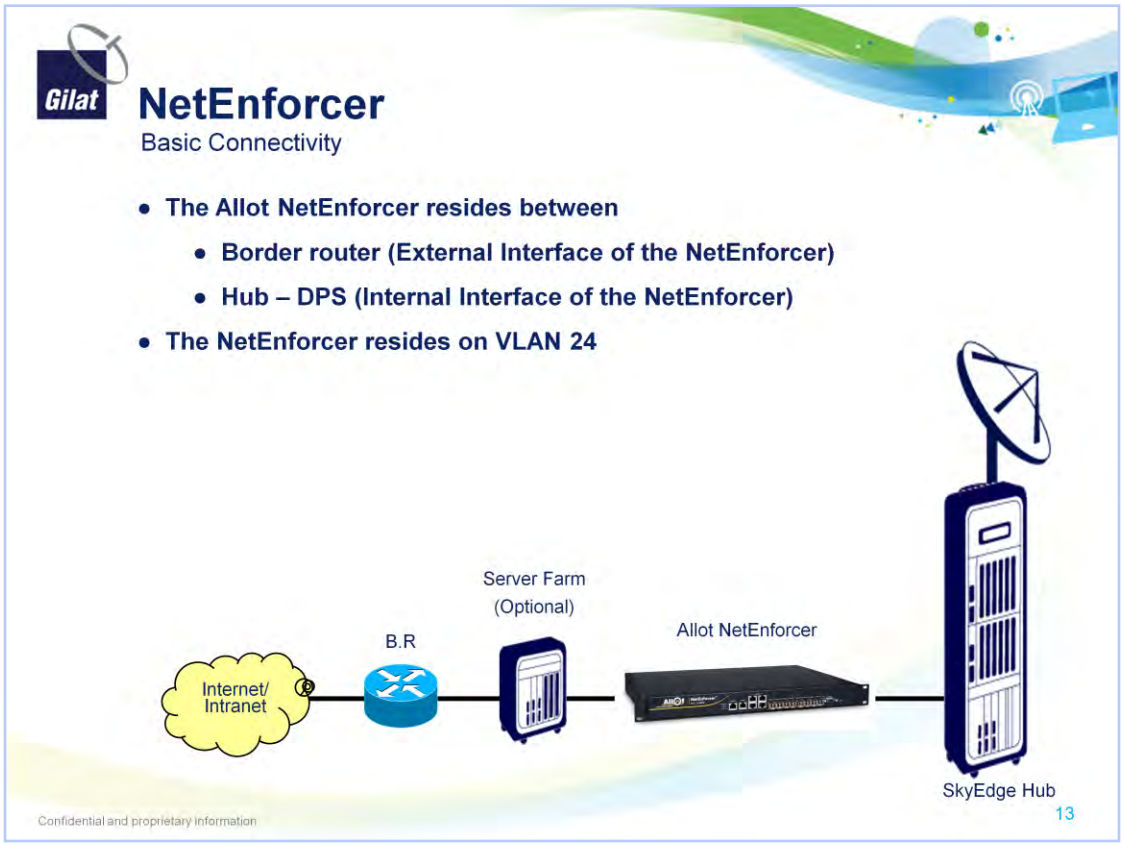
The diagram shows the basic Architecture of the NetXplorer system. The NetXplorer Server provides a centralized management system for all NetEnforcers on the network. The Configuration is done through the GUI client connected to the Server and then distributed to all the NetEnforcers.

A set of two NetEnforcers (one active and one redundant unit) is needed per Network Segment (NS).

Server Farm provides acceleration of the HTTP protocol. It is an optional component.

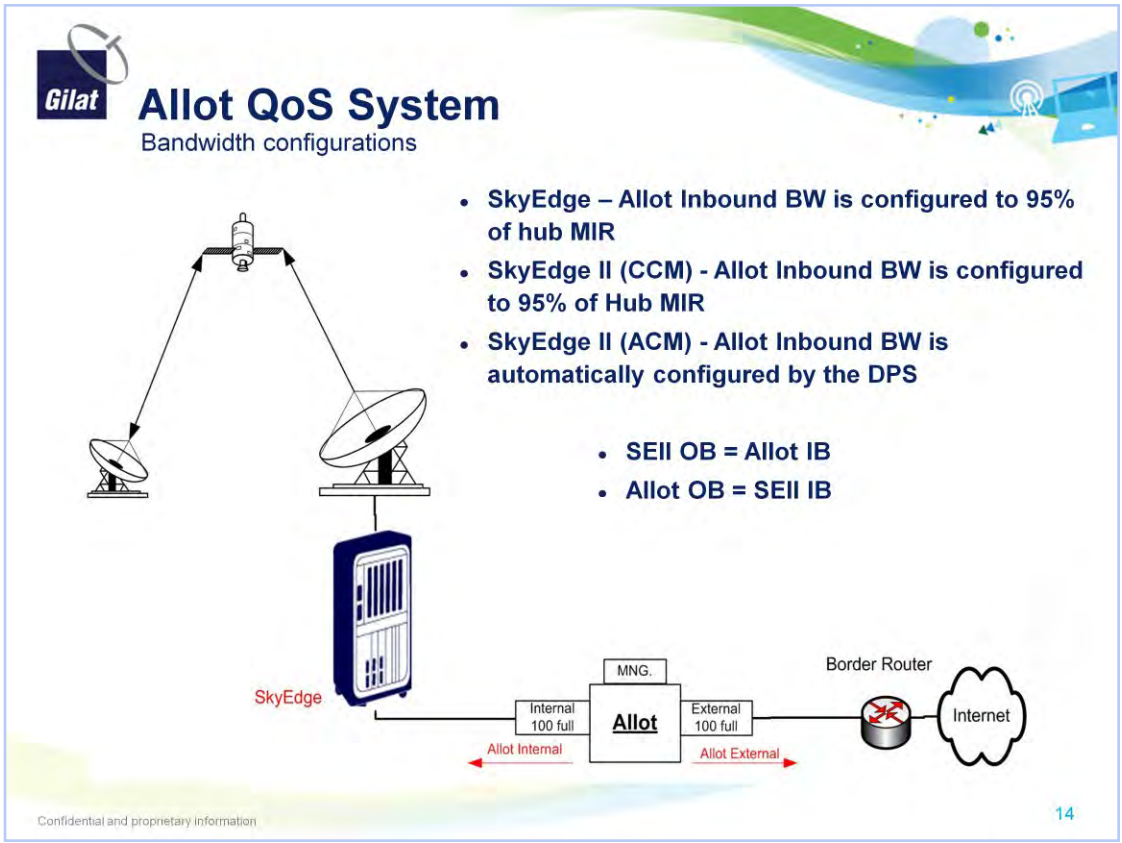
RPC – Remote PC (SkyEdge)

MPC – Management PC (SkyEdge II)

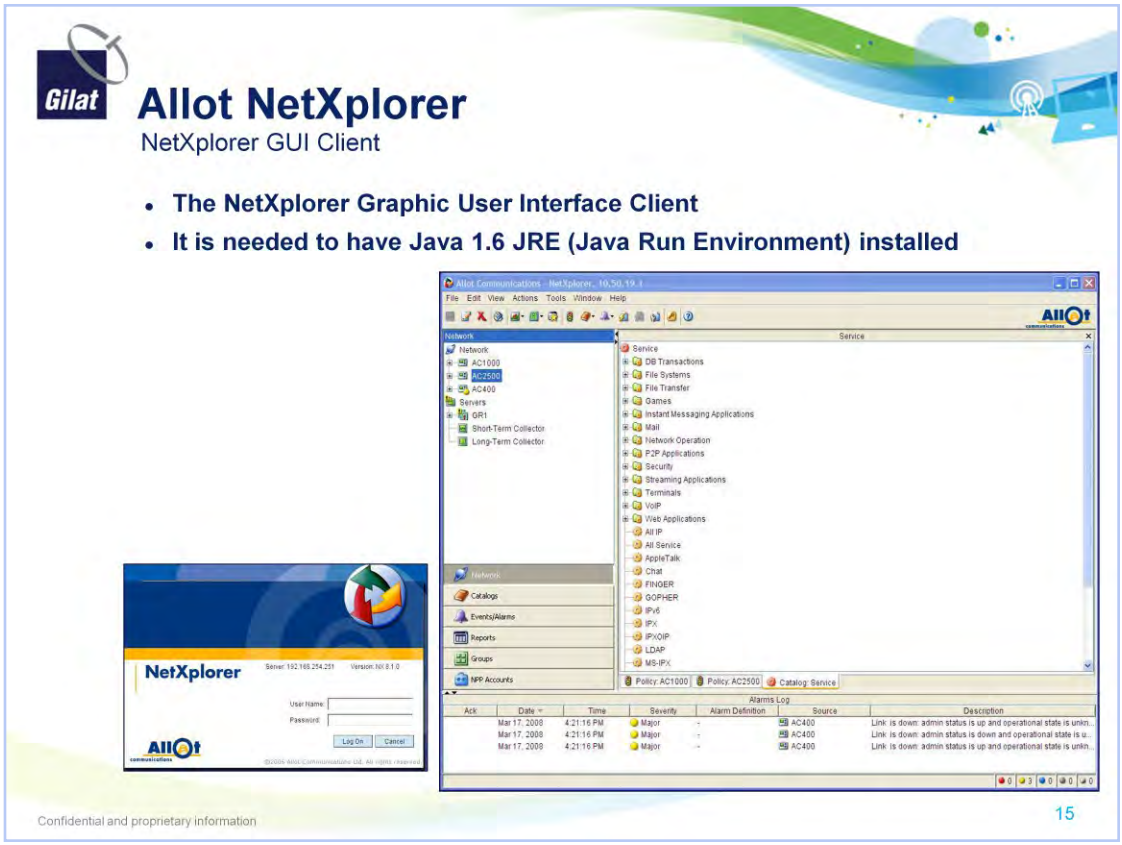


The diagram shows the logical connection between the NetEnforcer unit and the HUB (Internal Interface) and Border Router (External Interface).

The actual physical connection is done through switches, as shown in the previous slide.



Hub MIR: Maximum information rate supported by the Hub

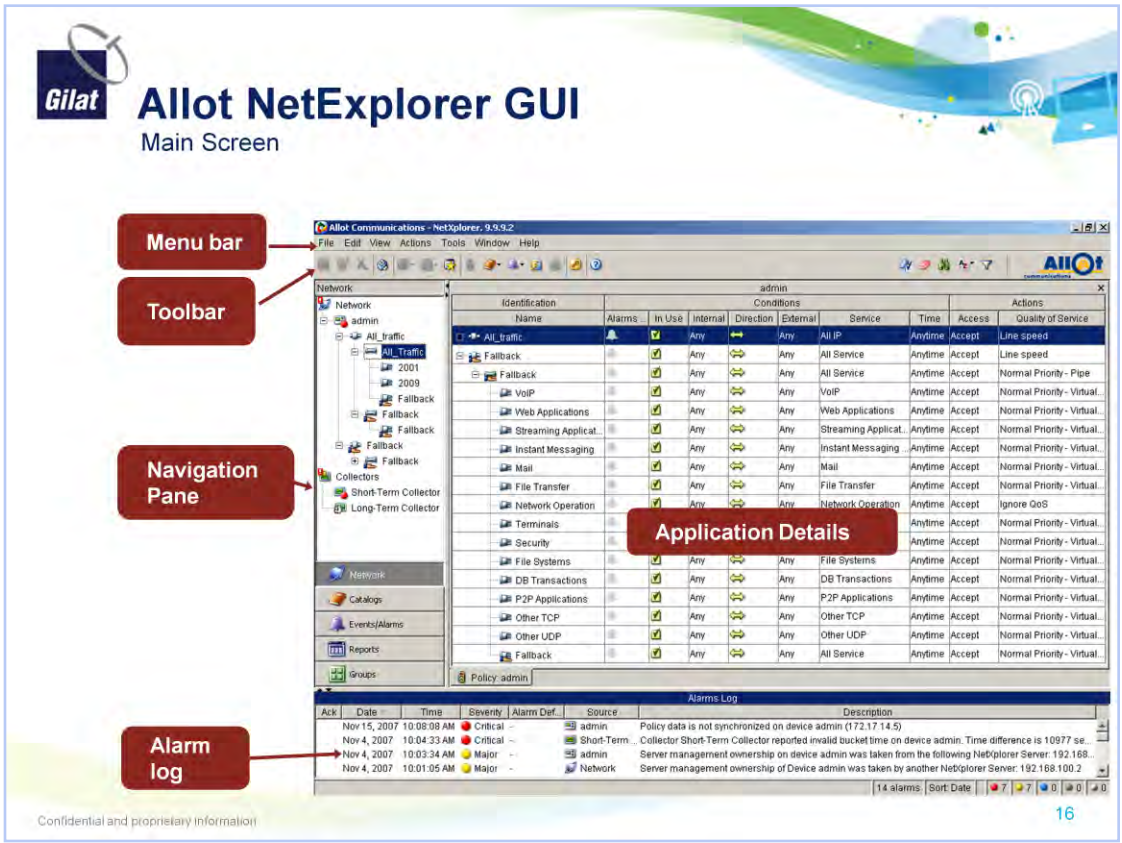


To connect to the NetXplorer GUI:

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:

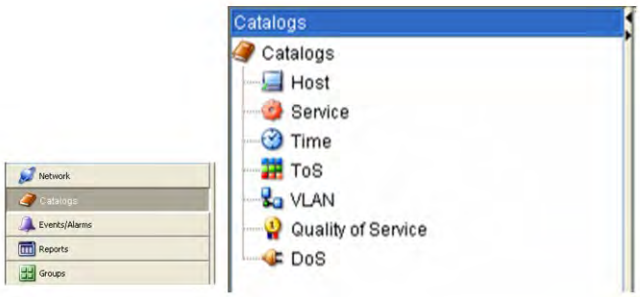
The Alarms Log displays a list of the alarms triggered by the alarm definitions. The Alarms Log is automatically refreshed every 30 seconds. The severity of an alarm is indicated by the color of the icon (Info: light gray, Warning: dark gray; Minor: blue; Major: yellow; Critical: red). A checkmark in 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.


Gilat
QoS Policy Configuration
17

QoS Policy Configuration

Catalogs

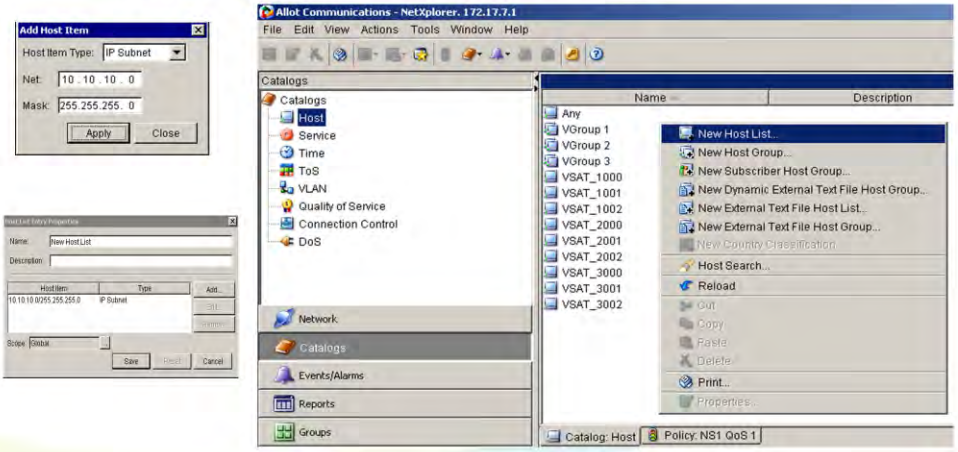
- **Catalogs represent objects to be used to build a QoS policy**
  - A QoS policy is applied to Objects that were previously defined in the catalog, thereby defining the classifications and actions for the policy



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



Example of Hosts:

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

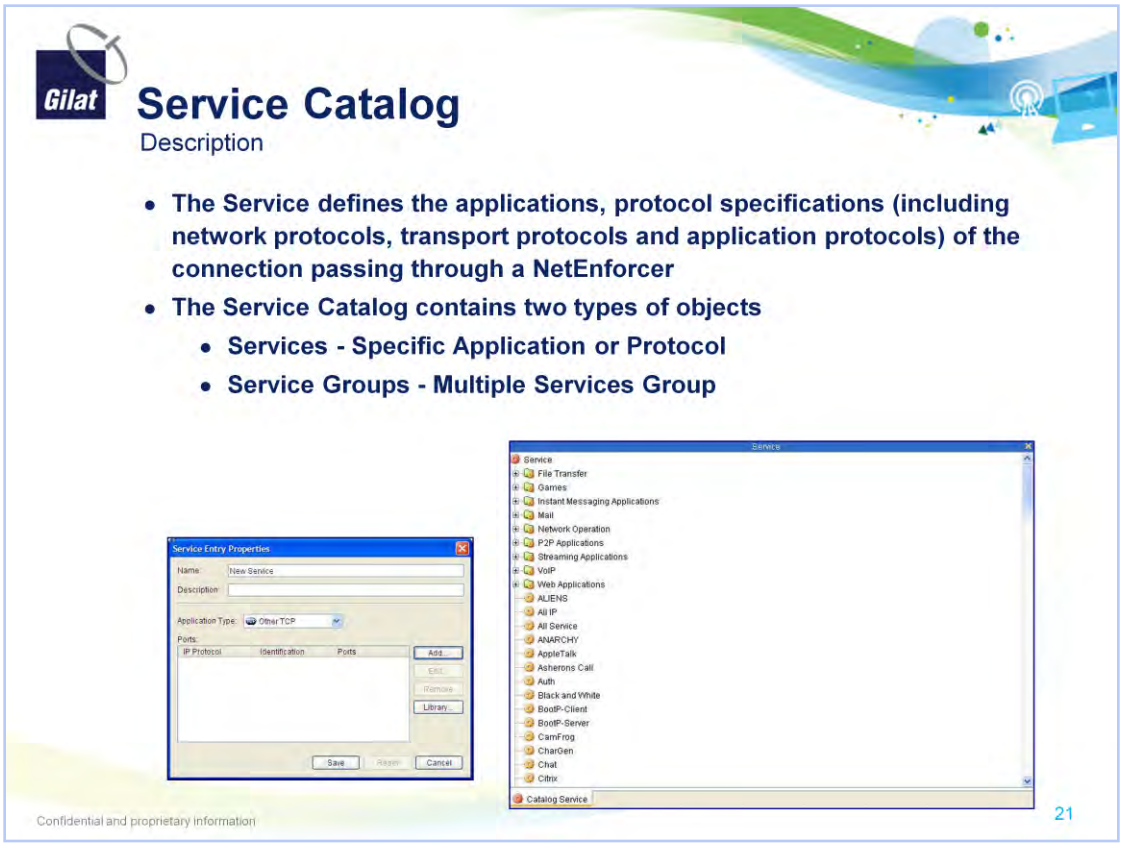
IP Subnet: For example, 10.10.10.0 with a subnet mask of 255.255.255.0.

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

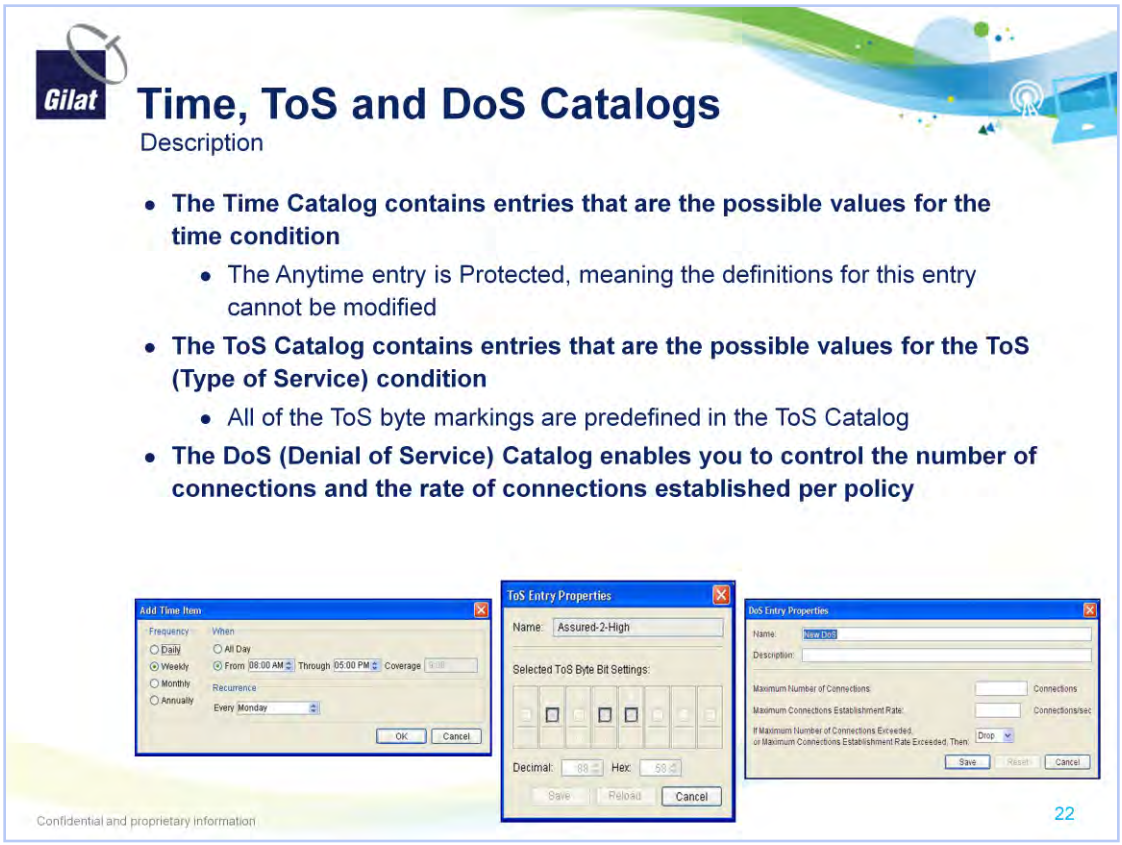
Description

- **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



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.

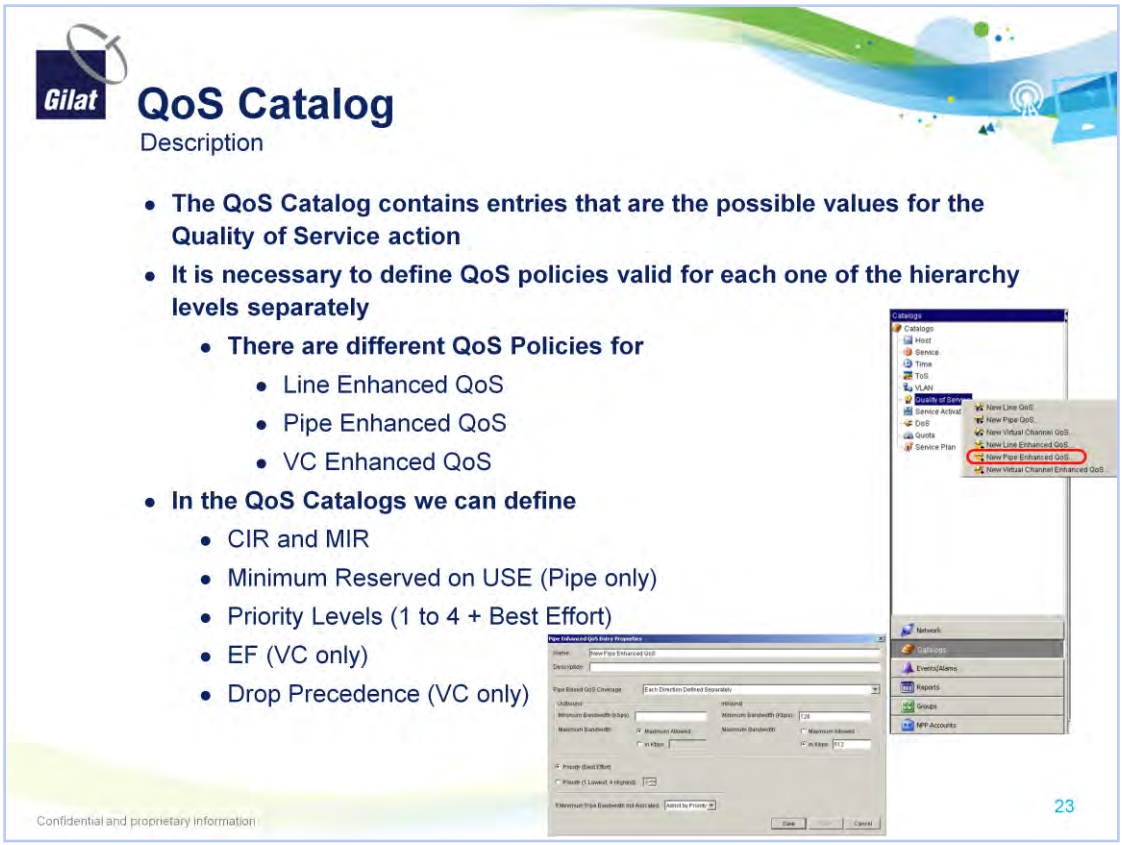
Service Groups enable you to efficiently assign policies to multiple services, instead of having to define separate policies on a service-by-service basis. Service groups also enable you to generate reports for specific groups of services.



Time 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 header s 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.



In NetEnforcer machines of version AC-1440 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. You can prioritize connections and specify minimum and maximum bandwidth per Pipe/Virtual Channel or per individual connection, and you can specify traffic-shaping techniques (CBR or Burst) for Virtual Channels.

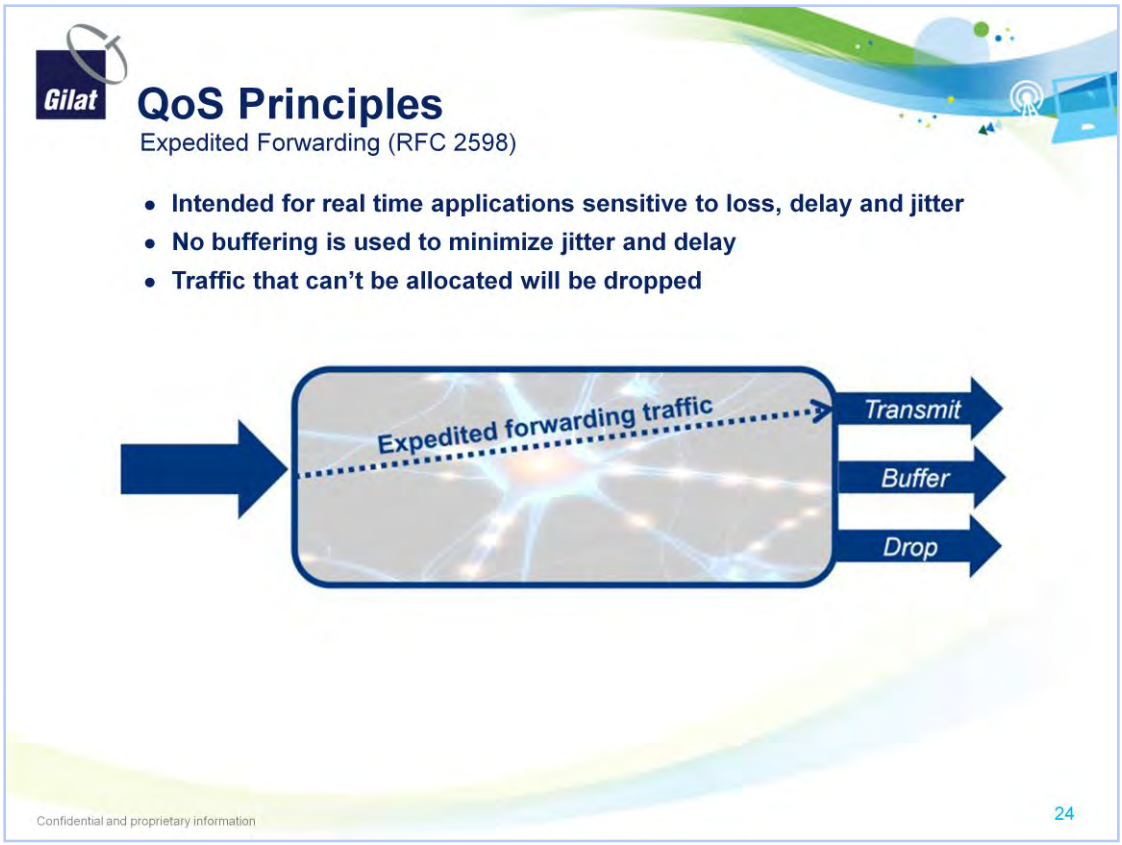
It is possible to configure the action to be taken if minimum bandwidth is not allocated, by selecting one of the following options from the designated dropdown list:

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.



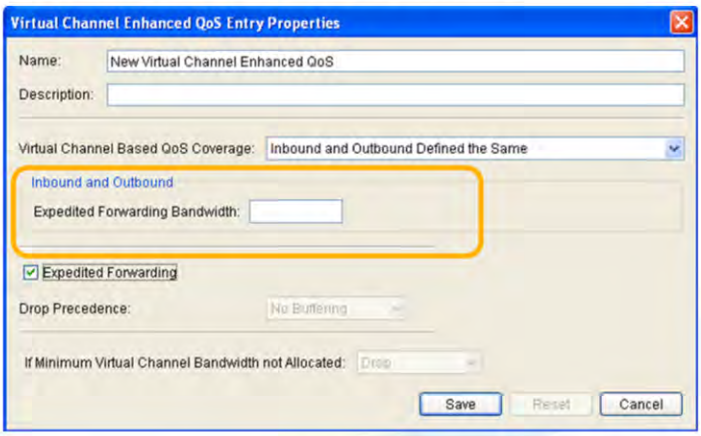
Expedited forwarding enables first-class service level for real time traffic which is loss-sensitive, delay-sensitive and jitter-sensitive and can also handle traffic bursts efficiently. With this feature users can ensure QoE for real-time applications such as VoIP and Videoconferencing services. Allot's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

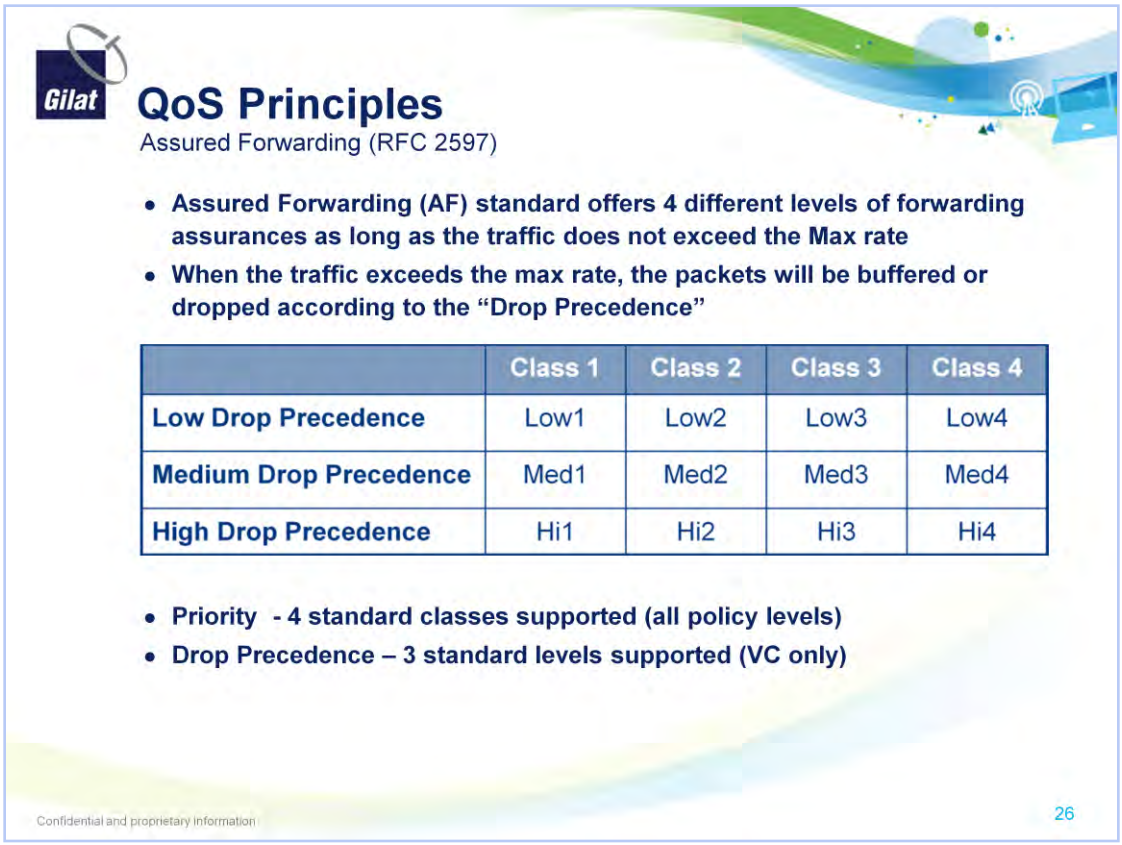
Expedited forwarding traffic (unlike traffic for which a regular "maximum" is defined) is not smoothed. Unlike traffic for which a regular maximum is defined, the Expedited forwarding defined rate can be allocated entirely in the first millisecond (burst). When starting to transmit in the middle of the 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.

QoS Principles

Expedited Forwarding (RFC 2598)

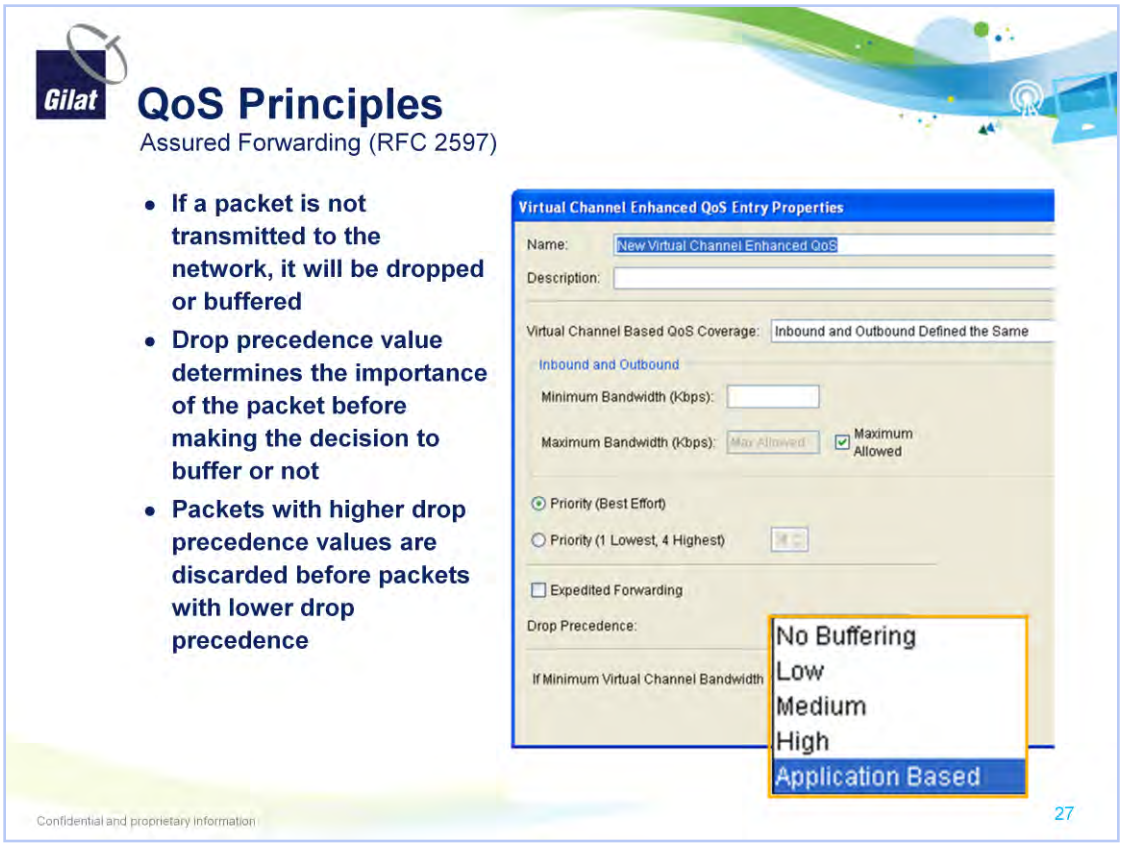
- **Definitions**
  - BW defined in kbps
  - Minimum = Maximum
  - Available only from Enhanced VC QoS catalog





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.

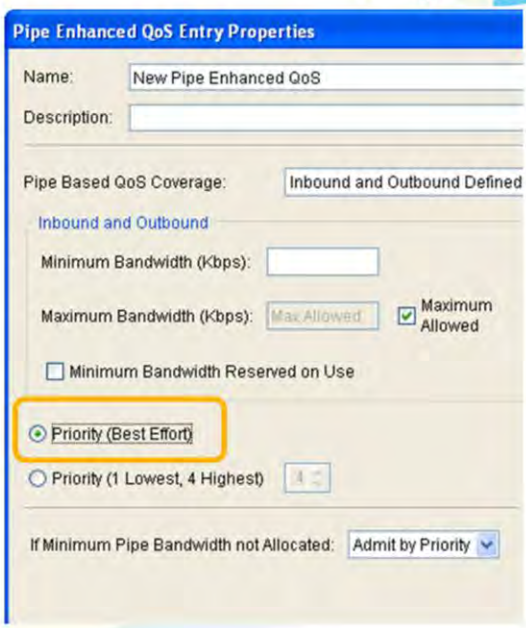


The default drop precedence value is “Application Based”, whereby high, medium and low values are pre-defined in the software code per application type.

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



28

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).

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

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**

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

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

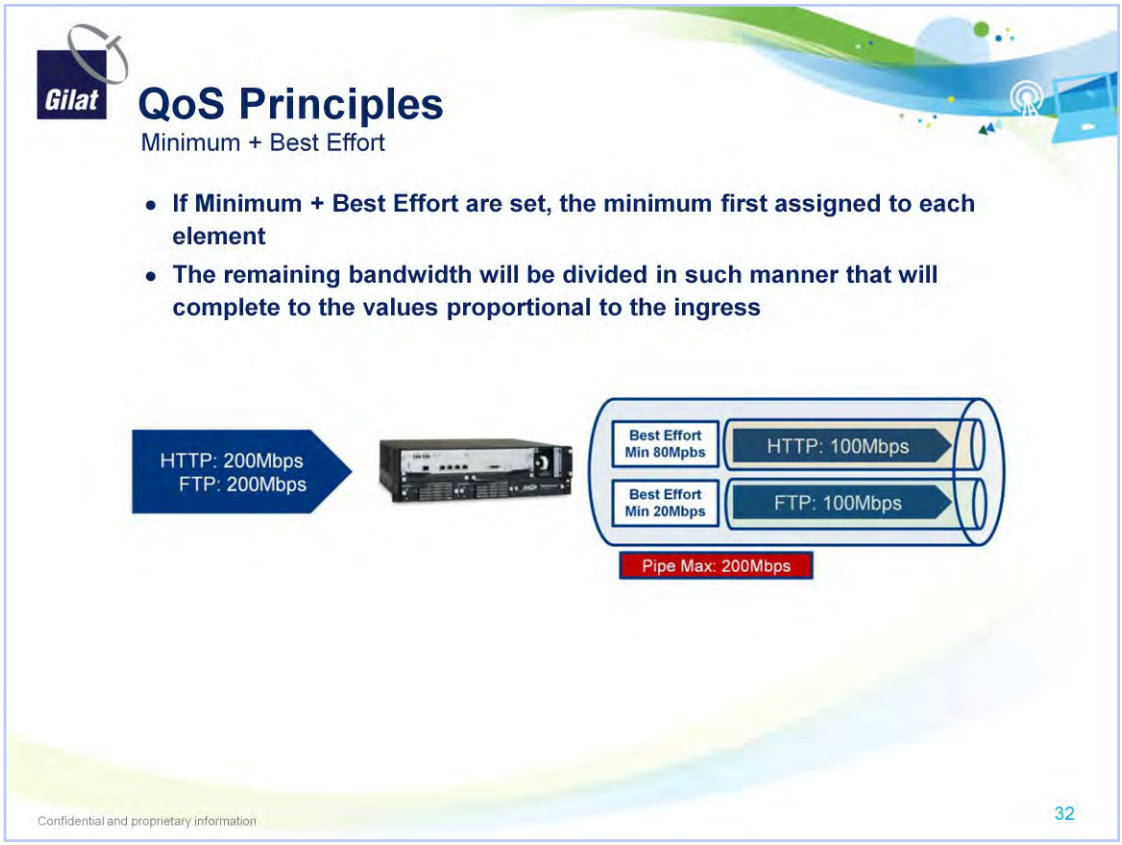
Remaining Bandwidth after min. allocation = Total Bandwidth Available – (Total Minimum)

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

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

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

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



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 Options

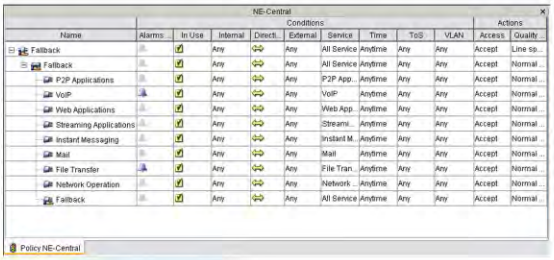
Regular (Legacy) vs Enhanced

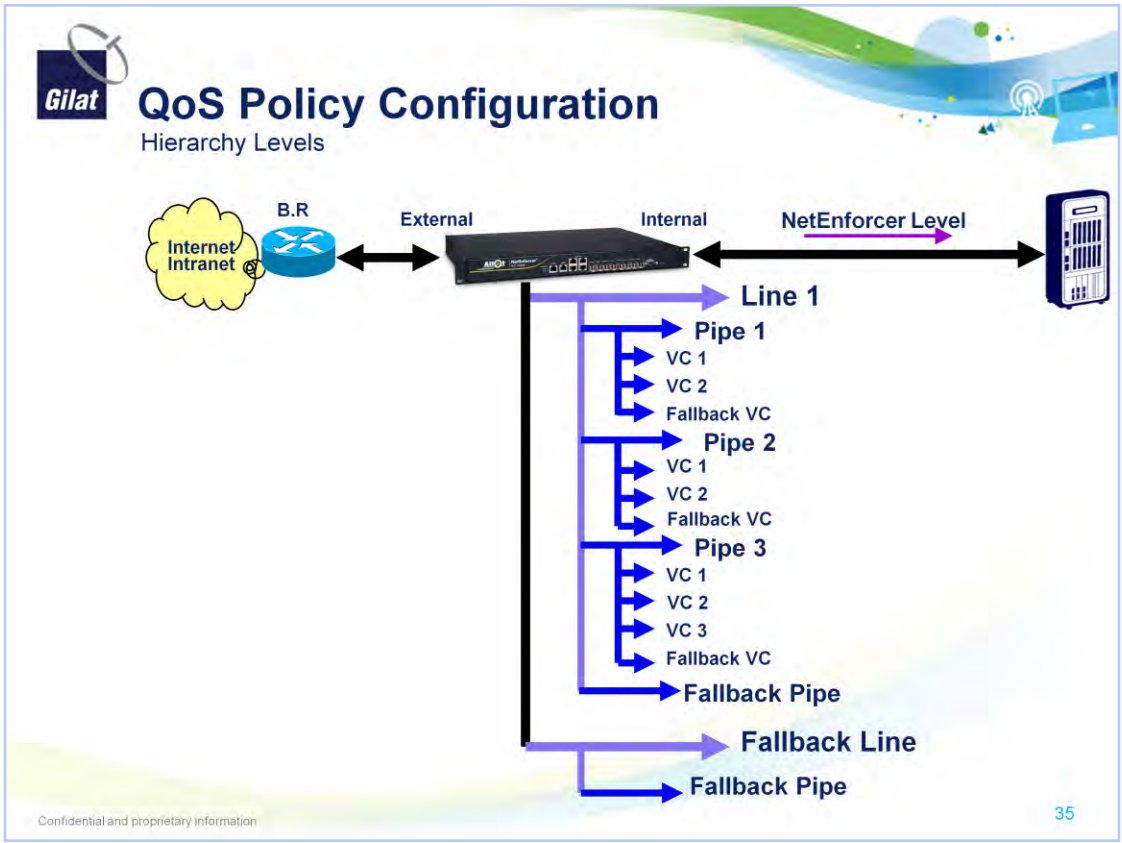
QoS Option	Regular			Enhanced		
	Line	Pipe	VC	Line	Pipe	VC
Definition per direction	Yes	Yes	Yes	Yes	Yes	Yes
Maximum (MIR)	Yes	Yes	Yes	Yes	Yes	Yes
Minimum (CIR)	Yes	Yes	Yes	Yes	Yes	Yes
Minimum Reserved on Use (CBR)	No	Yes	No	No	Yes	No
If Minimum not allocated	Yes	Yes	Yes	Yes	Yes	Yes
Per connection – burst/CBR	No	No	Yes	No	No	No
Priority Levels	10 (Pr. 1 for P2P)			4 + Best Effort		
Expedited Forwarding	No	No	No	No	No	Yes
Drop Precedence	No	No	No	No	No	Yes
Access Control	Reject			Bypass		

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)





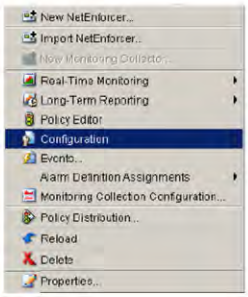
Fallback of any level can not be deleted.

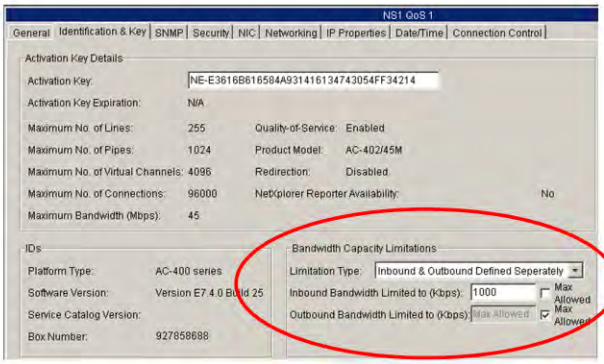
The action for Fallback of any level can be modified.

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

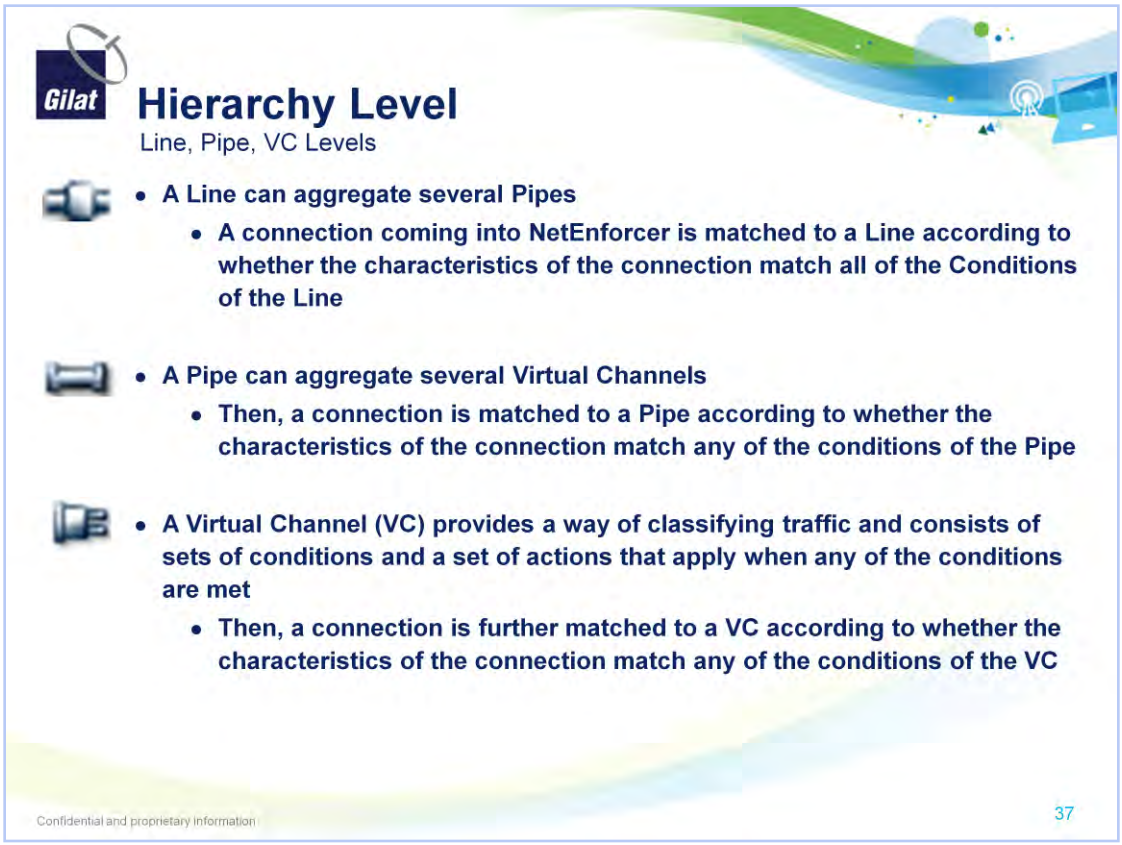




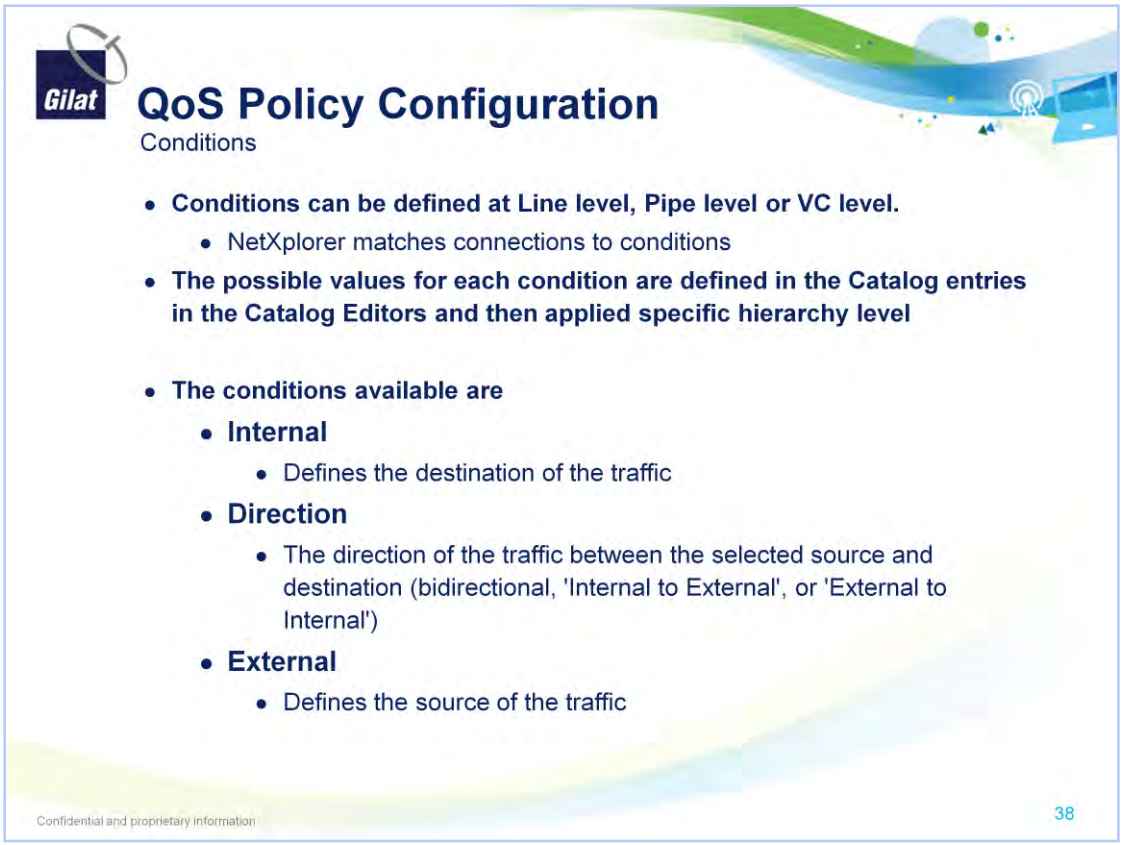
In SkyEdge the NetEnforcer Level is assigned to approximately 95% of the HUB MIR.

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.



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.



As soon as a Line Condition is found to match the connection, NetEnforcer stops looking at Lines. Similarly, within the matched Line, as soon as a Pipe Condition is found to match the connection, NetXplorer looks no further.

QoS Policy Configuration

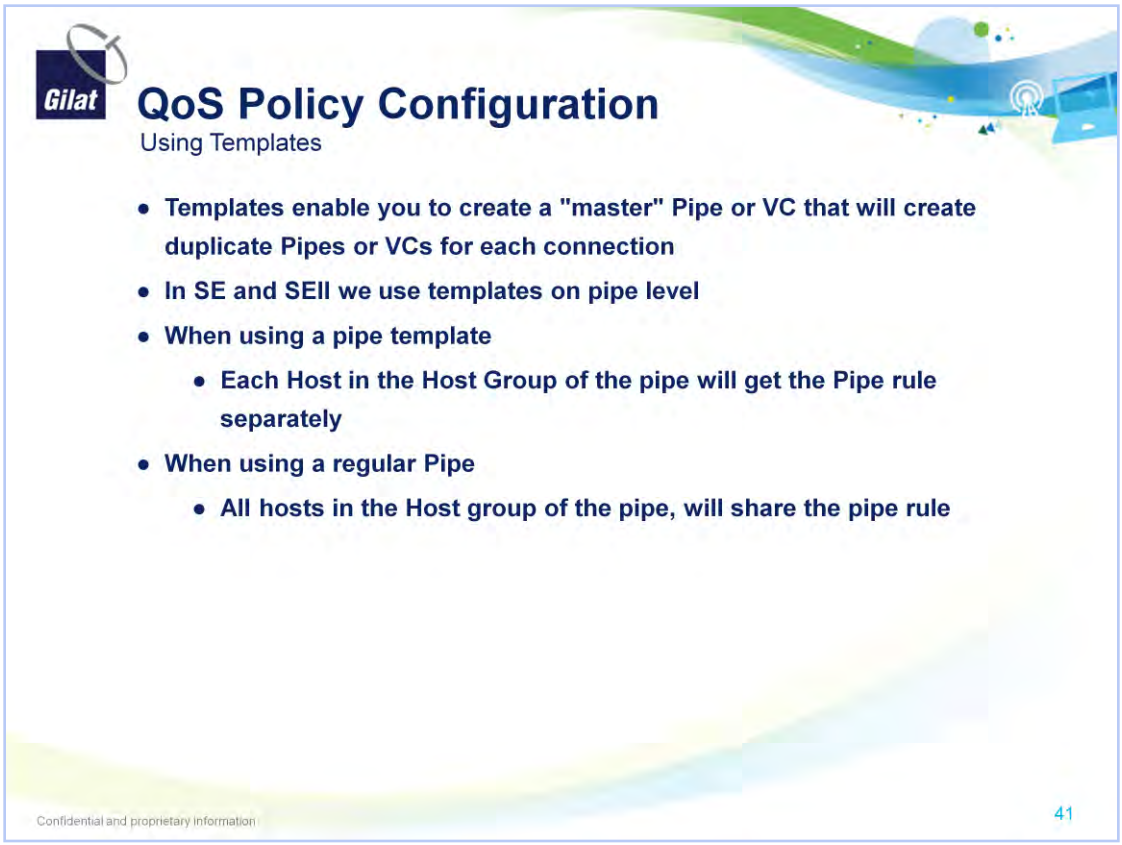
Conditions

- **Service**
  - **Defines the protocols relevant to a connection**
- **Time**
  - **Defines the time period during which the traffic is received.**
- **ToS**
  - **Defines the ToS byte contained in the IP headers of the traffic.**
- **VLAN**
  - **Defines VLAN traffic classification according to VLAN ID (VLAN Identifier) tags**

QoS Policy Configuration

Actions

- **Lines, Pipes and VCs are a set of actions that are enforced on traffic according to conditions that were defined for them**
- **Four actions can be defined for a Line, Pipe or Virtual Channel**
  - **Access Control**
    - Determines the access given to traffic
    - It is possible to Accept, Bypass or Drop connections
  - **QoS (Quality of Service)**
    - This action determines the QoS enforced on the traffic
  - **ToS Remarking**
    - NetEnforcer remark the ToS byte contained in the IP headers of the packets passing through it
  - **DoS (Denial of Service)**
    - Enables you to limit the frequency and number of connections



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

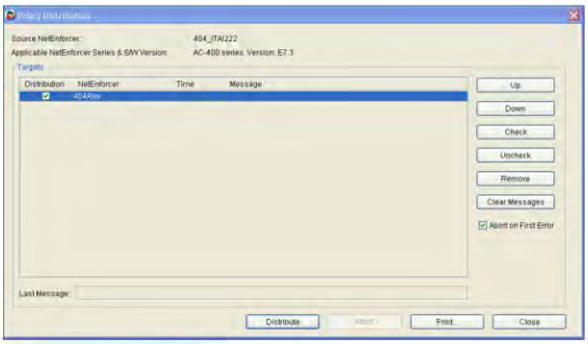
- **Using the Policy Distribution feature it is possible to update the policies of one unit and then distribute the new policies to other NetEnforcer units on the Network**
- **All NetEnforcers must be of the same Series and running the same major software version**

To distribute Policies:

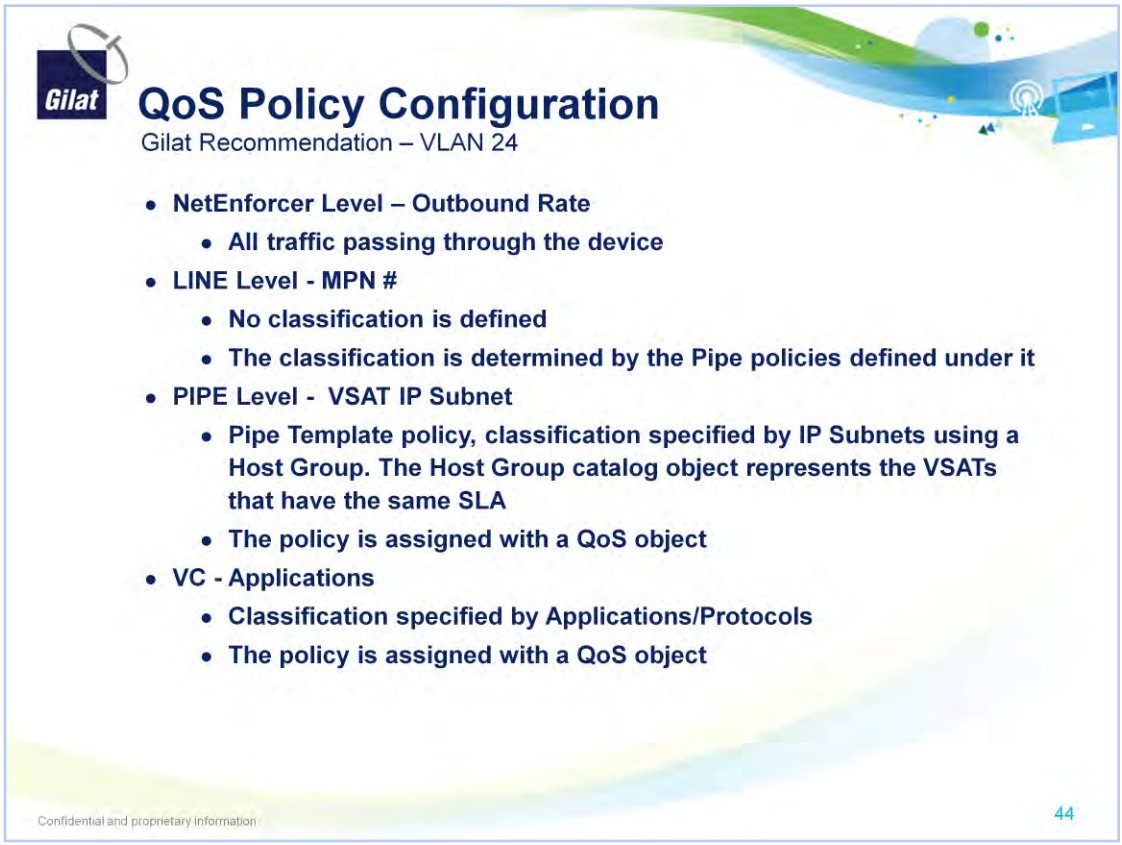
In the Navigation pane, right-click a NetEnforcer in the Navigation tree and select Policy Distribution from the popup menu.

OR

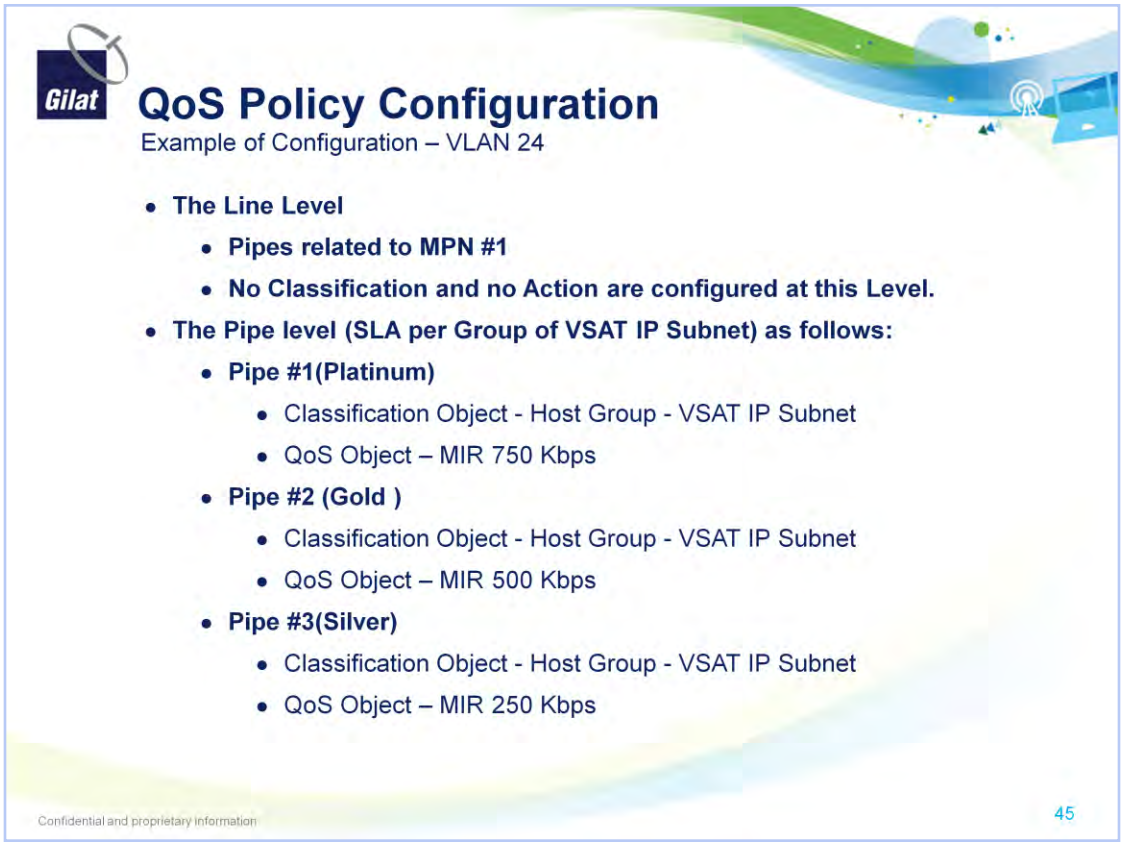
Select a NetEnforcer in the Navigation tree and then select Policy Distribution from the View menu.




Gilat
Gilat Recommended Configuration
43



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



In VSAT (IP Subnet) template case:
In a situation that VSAT serves a single network behind network.

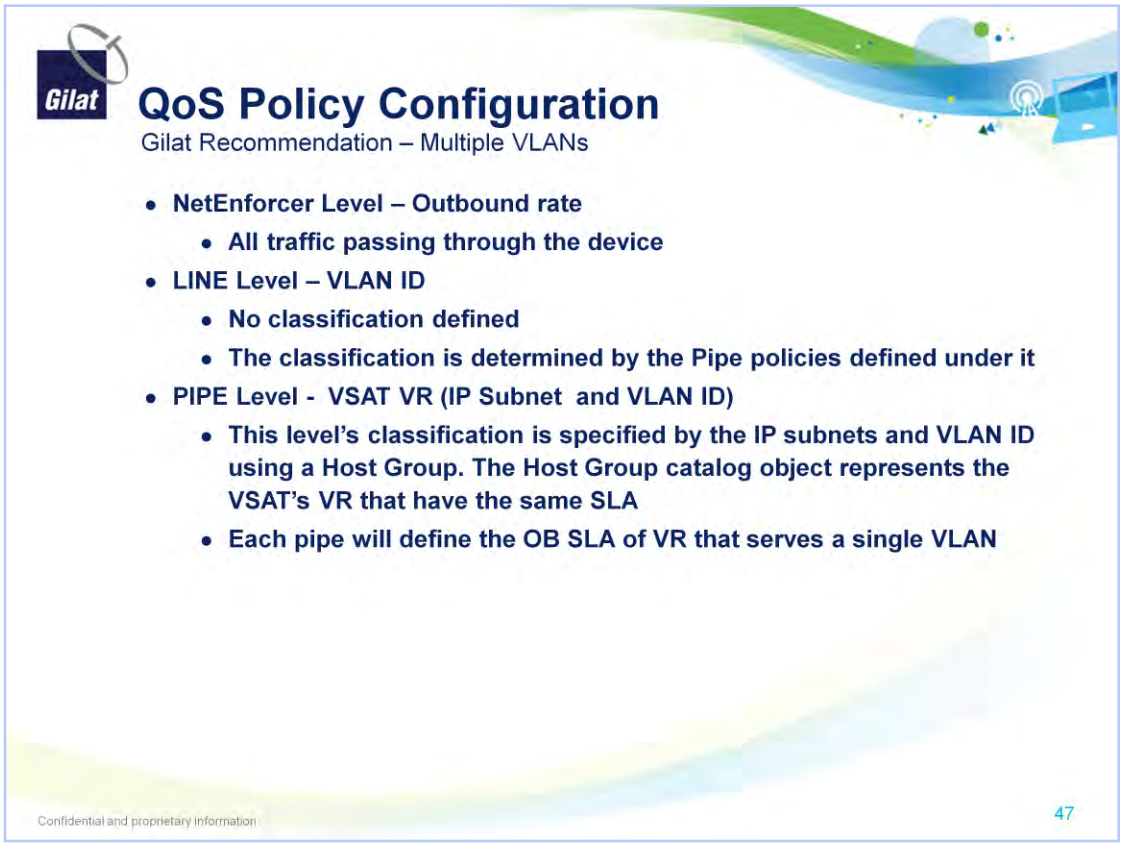
This level's classification is specified by the IP subnets that belong to a Host Group. The Host Group catalog Object represents VSATs with the same SLA.

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 12345- priority 3
  - **VC #3**
    - QoS Object for HTTP - priority 2
  - **VC #4**
    - QoS Object for FTP - priority 1



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

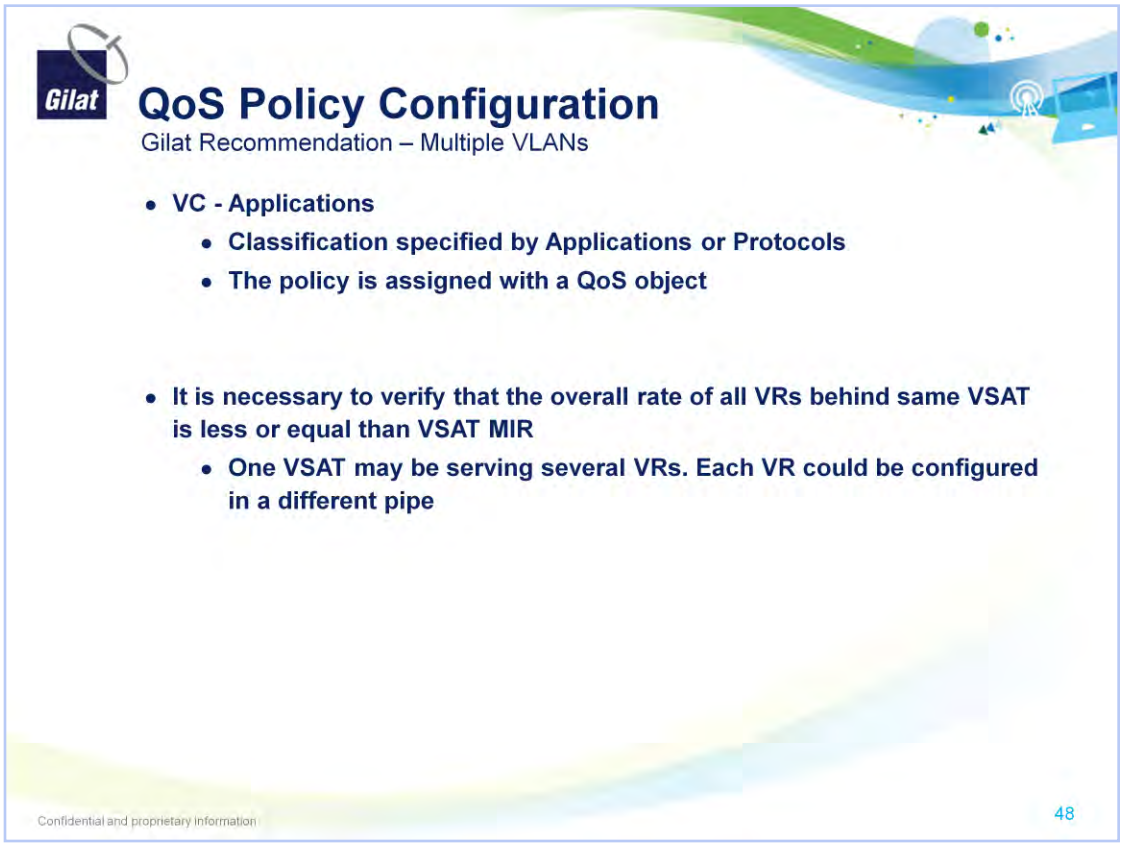
Pipe Configuration:

In VSAT VR (VSAT Virtual Router) template case:
In a situation the VSAT serves multiple networks behind network.

Each pipe will define the OB SLA of VR that is part of the VSAT VR and serves a single VLAN.

This level's classification is specified by the IP subnets and VLAN ID that belong to a specific VR. The VR catalog Object represents VR with the same SLA.

The Pipe policy is applied to a QoS object.



Since we are defining Pipes for VRs in this case, we must verify all the Pipes in the same VSAT can be served according to the QoS rule.

QoS Policy Configuration

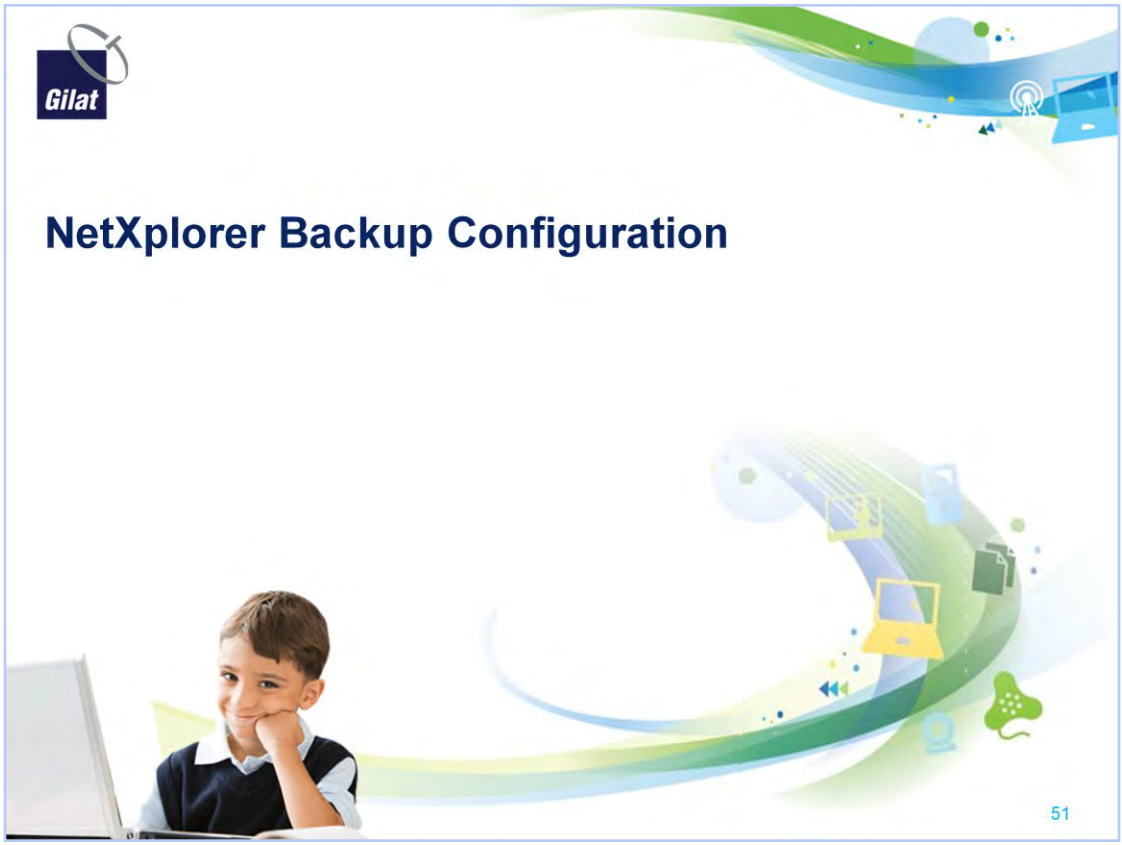
Example of Configuration – Multiple VLANs

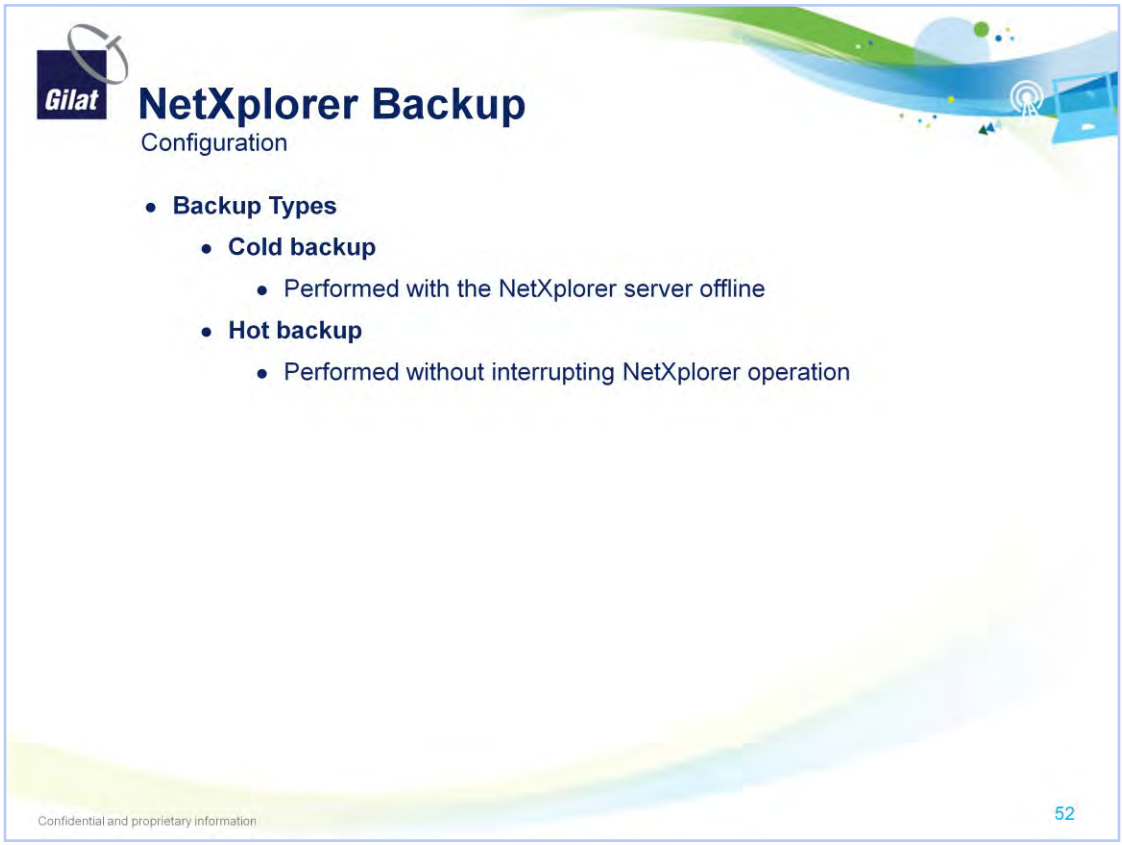
- **The Line Level**
  - **Pipes related to VLAN ID**
  - **No Classification and no Action are configured at this Level**
- **The Pipe level (SLA per Group of VSAT VR) as follows**
  - **Pipe #1(Platinum)**
    - Classification Object - Host Group - VSAT IP Subnet and VLAN ID
    - QoS Object - MIR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

QoS Policy Configuration

Example of Configuration – Multiple VLANs

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

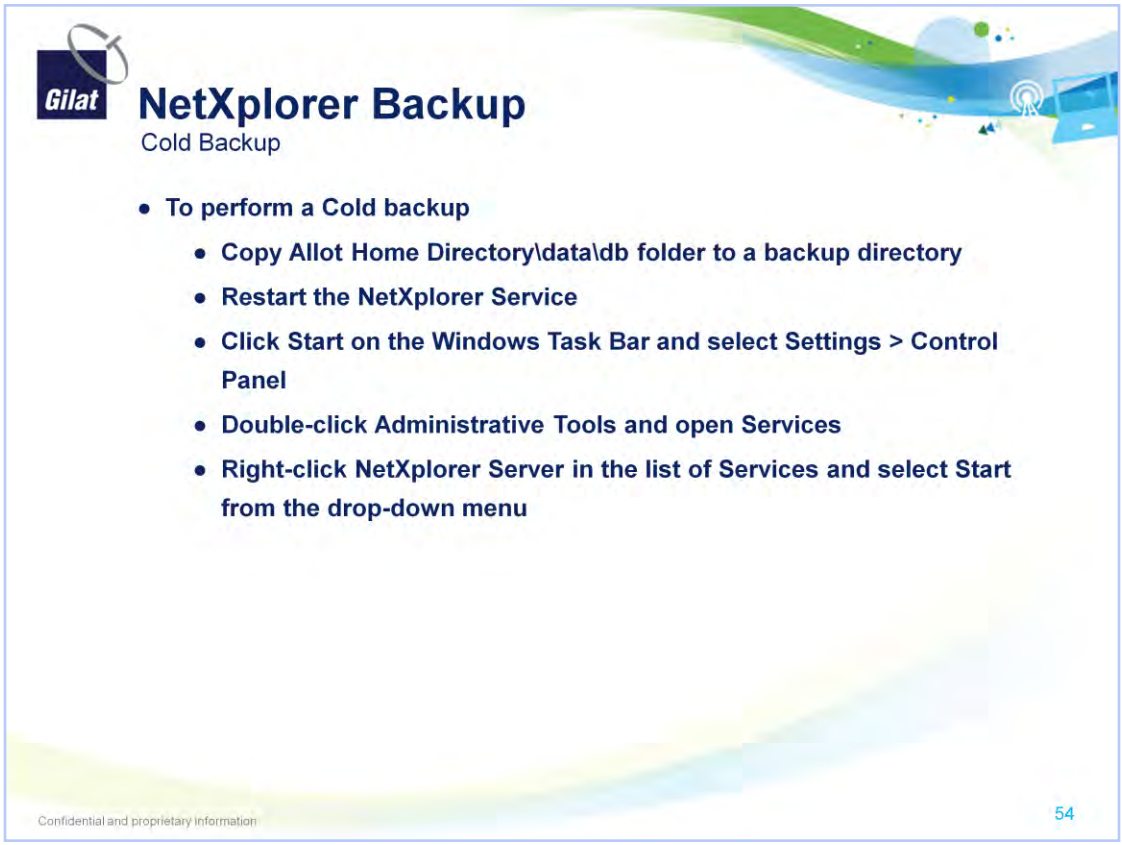

Gilat
NetXplorer Backup Configuration
51

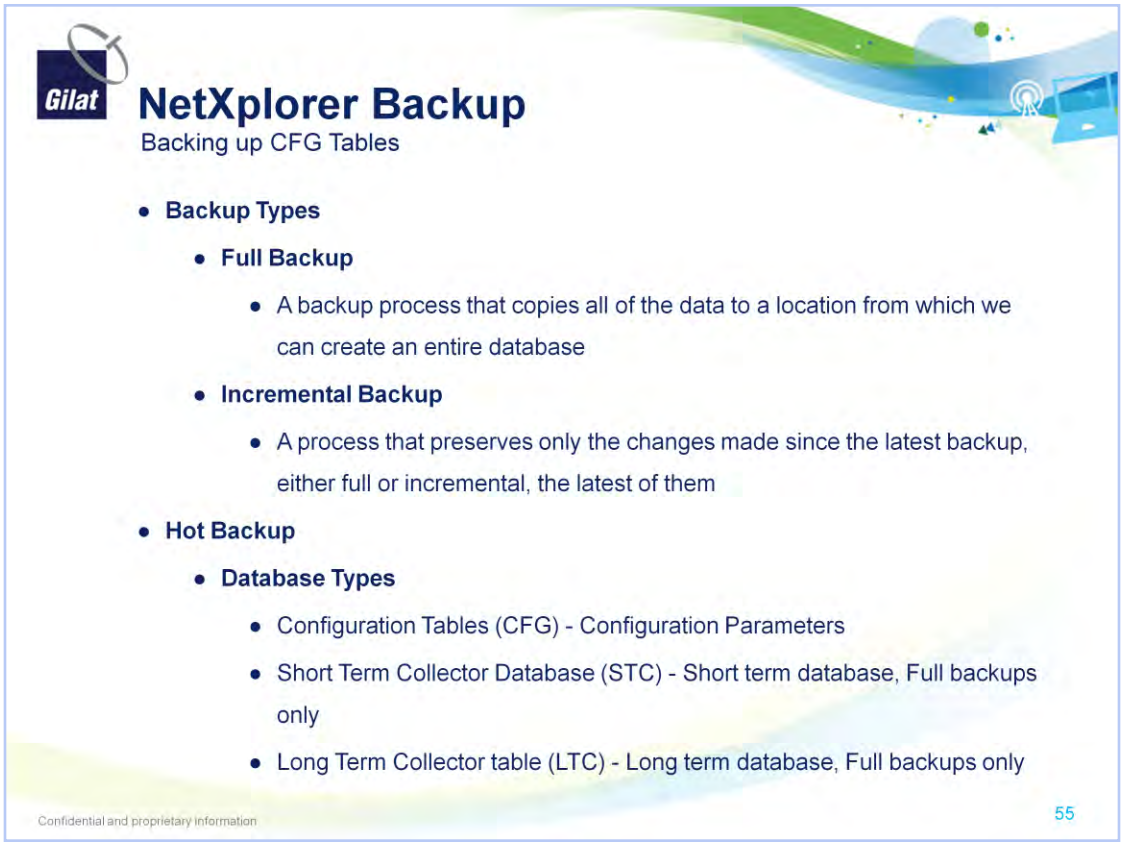

Gilat
NetXplorer Backup
Configuration
Backup Types
Cold backup
Performed with the NetXplorer server offline
Hot backup
Performed without interrupting NetXplorer operation
Confidential and proprietary information
52

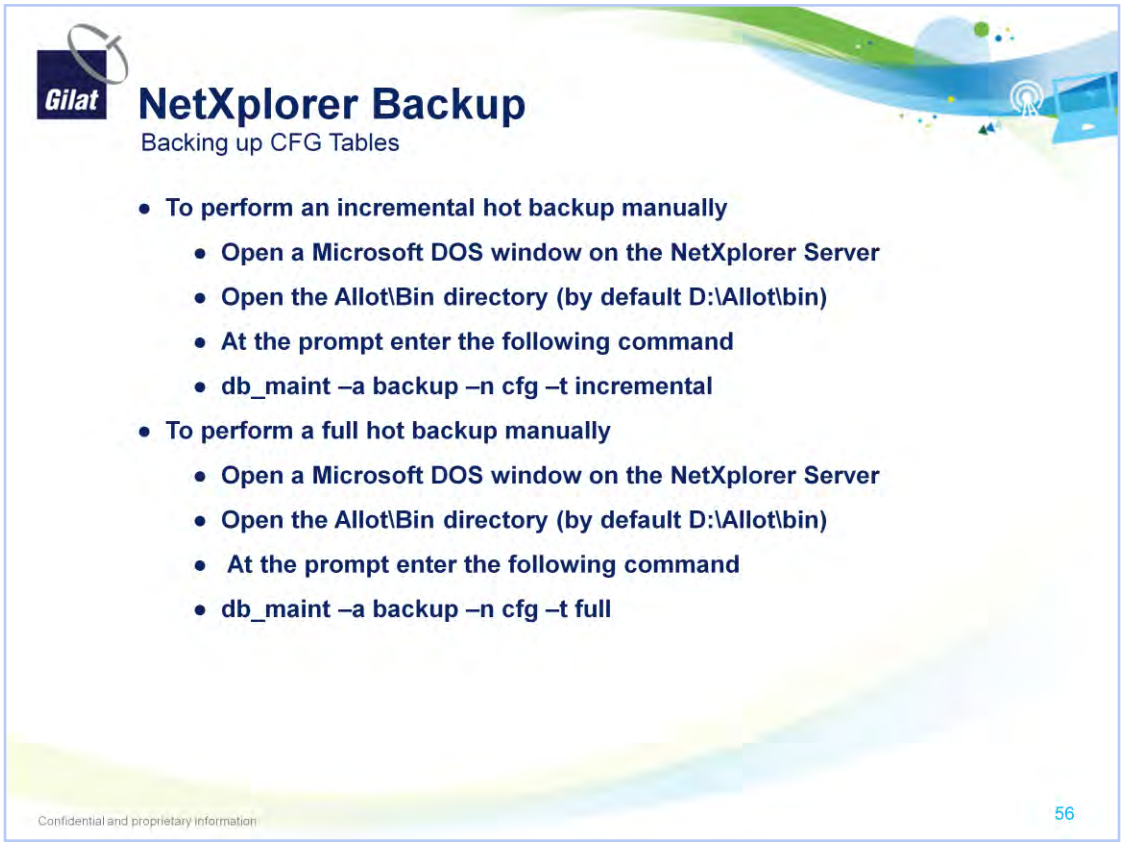
NetXplorer Backup

Cold Backup

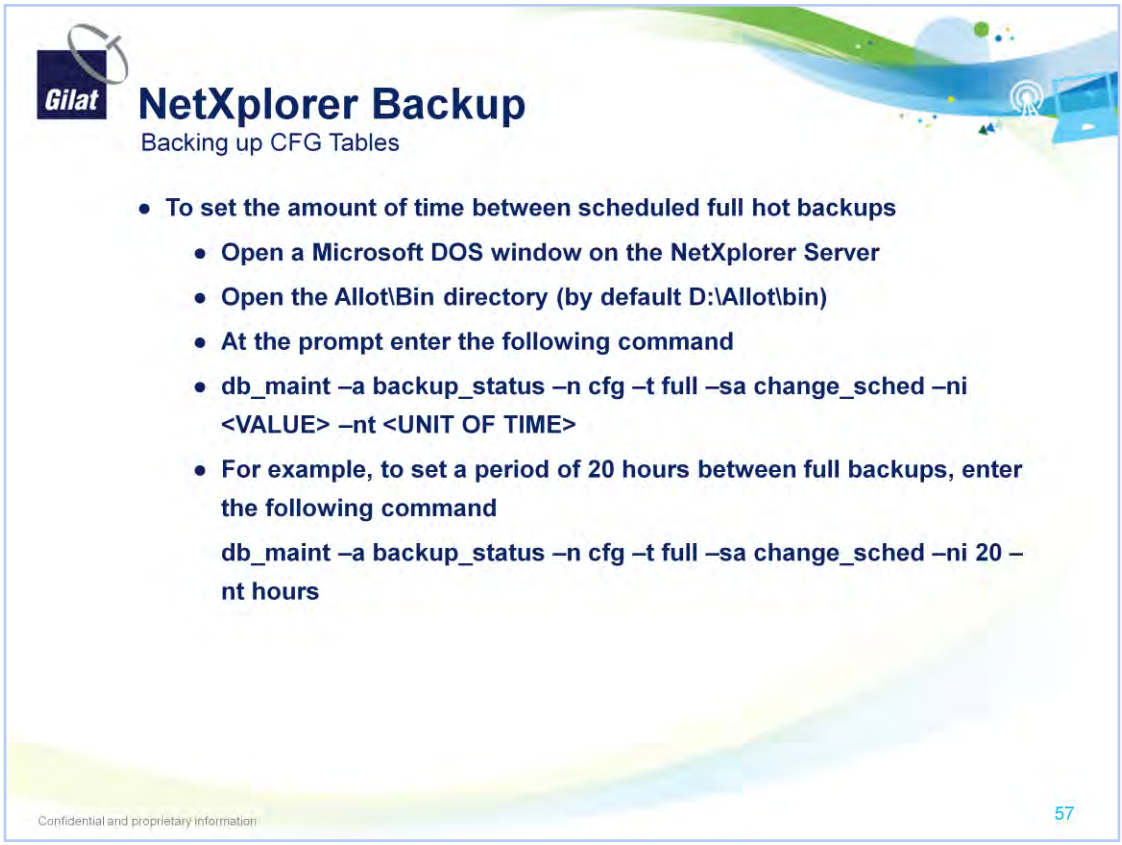
- To perform a Cold backup
  - Stop the NetXplorer Service
  - Click Start on the Windows Task Bar and select Settings > Control Panel
  - Double-click Administrative Tools and open Services
  - Right-click NetXplorer Server in the list of Services and select Stop from the drop-down menu
  - Check the allot_ltc.txt, allot_stc.txt log files located under Allot Home Directory\Logs in order to verify that NetXplorer services are not running: The following lines should appear in both allot_ltc.txt, allot_stc.txt log files: "Disable all events" "End of current events"


Gilat
NetXplorer Backup
Cold Backup
To perform a Cold backup
Copy Allot Home Directory\data\db folder to a backup directory
Restart the NetXplorer Service
Click Start on the Windows Task Bar and select Settings > Control Panel
Double-click Administrative Tools and open Services
Right-click NetXplorer Server in the list of Services and select Start from the drop-down menu
Confidential and proprietary information
54


Gilat
NetXplorer Backup
Backing up CFG Tables
Backup Types
Full Backup
A backup process that copies all of the data to a location from which we can create an entire database
Incremental Backup
A process that preserves only the changes made since the latest backup, either full or incremental, the latest of them
Hot Backup
Database Types
Configuration Tables (CFG) - Configuration Parameters
Short Term Collector Database (STC) - Short term database, Full backups only
Long Term Collector table (LTC) - Long term database, Full backups only
Confidential and proprietary information
55



The commands should not be cut and pasted into the DOS window, but typed in. They may not function properly unless entered manually.



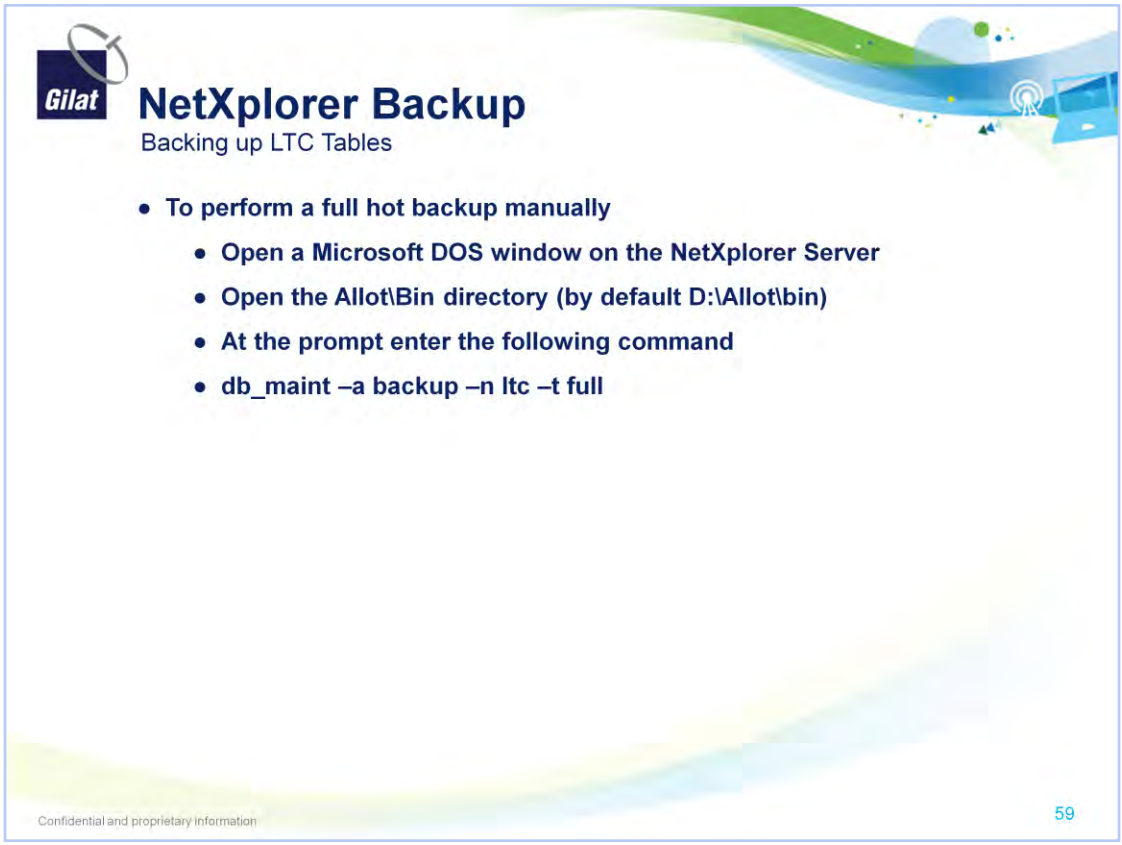
The commands should not be cut and pasted into the DOS window, but typed in. They may not function properly unless entered manually.

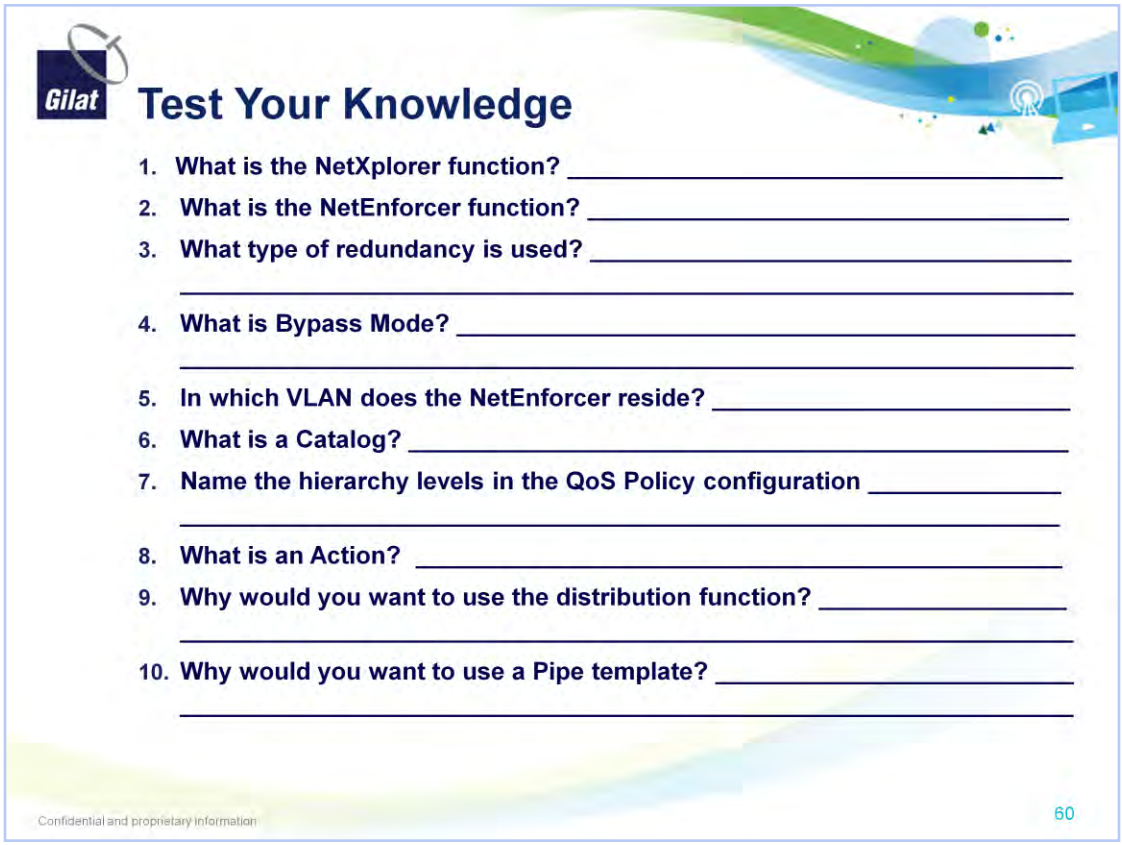
NetXplorer Backup

Backing up STC Tables

- To perform a full hot backup manually
  - Open a Microsoft DOS window on the NetXplorer Server
  - Open the Allot\Bin directory (by default D:\Allot\bin)
  - At the prompt enter the following command
  - db_maint –a backup –n stc –t full
- To set the amount of time between scheduled full hot backups
  - Open a Microsoft DOS window on the NetXplorer Server
  - Open the Allot\Bin directory (by default D:\Allot\bin)
  - At the prompt enter the following command
  - db_maint –a backup_status –n stc –t full –sa change_sched –ni <VALUE> –nt <UNIT OF TIME>
  - For example, to set a period of 20 hours between full backups, enter the following command

    db_maint –a backup_status –n stc –t full –sa change_sched –ni 20 –nt hours


Gilat
NetXplorer Backup
Backing up LTC Tables
To perform a full hot backup manually
Open a Microsoft DOS window on the NetXplorer Server
Open the Allot\Bin directory (by default D:\Allot\bin)
At the prompt enter the following command
db_maint –a backup –n ltc –t full
Confidential and proprietary information
59


Gilat
Test Your Knowledge
1. What is the NetXplorer function? _____
2. What is the NetEnforcer function? _____
3. What type of redundancy is used? _____
_____
4. What is Bypass Mode? _____
_____
5. In which VLAN does the NetEnforcer reside? _____
6. What is a Catalog? _____
7. Name the hierarchy levels in the QoS Policy configuration _____
_____
8. What is an Action? _____
9. Why would you want to use the distribution function? _____
_____
10. Why would you want to use a Pipe template? _____
_____
Confidential and proprietary information
60


Gilat
Thank You
Boundless Communications
61