# CLEAR-Flow


## Abstract

One of the fundamental limitations with most traffic monitoring and management methods in use today is that they are not built into the network itself. CLEAR-Flow represents a new paradigm for network traffic management. For the first time, CLEAR-Flow brings together network monitoring, analysis, and response in a single process inside the Ethernet switching fabric. This creates a powerful toolbox for solving diverse network challenges that were previously difficult or impossible to solve, such as threat detection in high-speed networks.

In this white paper we present an overview of the CLEAR-Flow technology, including the key benefits. Additionally, this paper provides an example of a security application that demonstrates CLEAR-Flow's value.

## Introduction

In 2009, the Cyber Secure Institute estimated that the Conficker/Downadup worm could have infected as many as 10 million computers worldwide, with total economic damage as high as $9.1 billion. The 2009 CSI Computer Crime and Security Survey[1] found that 29% of respondents reported denial-of-service (DoS) incidents and 64% reported malware infections. The Sapphire/Slammer worm scanned over 55 million IP addresses per second and infected 90 percent of vulnerable Internet hosts worldwide within 10 minutes. Worms and viruses will continue to become more destructive using faster algorithms while carrying more malicious payloads and Trojan horses.

Corporate IT professionals are struggling to understand the types of applications, security threats, and traffic trends affecting the network as enterprise networks have experienced increased traffic, size, and importance to business. Security threats, amplified by the increasing application and traffic mix, are appearing at an unprecedented rate and spreading world-wide within hours or even minutes—with the financial impact of these attacks reaching billions of dollars.

Combating these security threats requires examination of every packet traversing the enterprise—an approach that clearly does not scale to today's high speed, 10 gigabit networks. To better solve this problem, Extreme Networks® has developed a traffic management technology—Continuous Learning, Examination, Action, and Reporting of Flows (CLEAR-Flow)—which is available on Summit® X450a, X450e, X480, and X650 series and all BlackDiamond series switches—brings new technology to bear on the problem of network monitoring by bringing new awareness to network switching hardware. This technology makes it possible to proactively identify anomalies in user, host, and application behavior.

CLEAR-Flow technology is ideally suited for a number of traffic management challenges, including:

- Network security—Intrusion detection, worm and virus containment, and Denial of Service (DoS) suppression
- Network management—Capacity planning, trending analysis, application classification, and Quality of Service (QoS) enforcement
- Network billing—Accounting and Service Level Agreement (SLA) enforcement

Early detection of threats such as viruses, worms and DoS attacks is one of the most important challenges facing corporate networks today. Successfully finding network threats requires searching through all network traffic looking for unusual packets. To date, network early warning systems such as Intrusion Detection Systems (IDS) have been unable to scale to meet the bandwidth and latency challenges of monitoring traffic in enterprise networks.

[1]2009 CSI Computer Crime and Security Survey, used with the permission of the Computer Security Institute

## CLEAR-Flow Basics

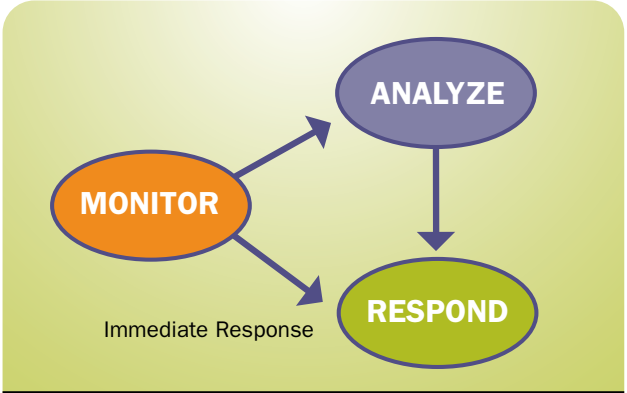



**Figure 1: CLEAR-Flow Processing Architecture**

CLEAR-Flow represents a new paradigm for network traffic management. For the first time, CLEAR-Flow brings together network monitoring, analysis, and response in a single process inside the Ethernet switching fabric. This creates a powerful toolbox for solving diverse network challenges that were previously difficult or impossible to solve, such as threat detection in high-speed networks.

One of the fundamental limitations with most traffic monitoring and management methods in use today is that they are not built into the network itself. Typically, these strategies use some sort of software on the switch to send traffic, summaries of traffic, or samples of traffic to a remote collection device. Regardless of the exact strategy used, the traffic sent to the monitoring station does not represent interesting or unusual traffic, but instead is an exact copy or summary of all the traffic on the network.

The problem with this strategy is that it simply does not scale. It is clearly impossible for the switch to forward a copy of each and every packet to an off-switch analyzer, and it is also impossible for any real-world analyzer to keep up with the flow. There are simply too many individual packets and flows for the embedded switch software to keep up.

The CLEAR-Flow approach is fundamentally different. CLEAR-Flow is a way for Ethernet switches to examine and forward data. Instead of simply looking at the source and destination of the traffic and forwarding it along the appropriate Layer 2 or Layer 3 path, CLEAR-Flow goes a step further by allowing network administrators to specify certain types of traffic that deserve more attention. Once certain criteria for this traffic are met, the switch can then either take an immediate, pre-determined action, or send a copy of the traffic for off-switch analysis. This analysis can, in turn, result in the appropriate response to the particular traffic, for example, blocking a DoS attack or rate-limiting a user in violation of his service level agreement.

Using these three steps—monitor, analyze, and respond—CLEAR-Flow provides a complete solution for detecting network events and trends, analyzing their significance to the network, and taking the appropriate response. A closer look at how CLEAR-Flow works, and how it can be used in some real-world scenarios, follows.

CLEAR-Flow processes all traffic through the following series of steps:

## Monitor

CLEAR-Flow uses hardware capabilities in the switch to scan and filter each packet as it passes through. CLEAR-Flow ignores any packets that are not of interest, and focuses only on the ones that meet the monitoring criteria set by the administrator. When it finds packets of interest, CLEAR-Flow uses another hardware feature—event counters—to track the occurrence. If immediate response is warranted, the hardware triggers the software to immediately change the way the traffic is handled by the switch.

» **Step 1—Filter**
Integrated into the Access Control mechanisms of the switch, special CLEAR-Flow classifiers look for match conditions as traffic traverses the switch at line rate. If the switch finds the specified traffic, it can immediately react to it, or increment a counter. CLEAR-Flow can look for up to 112,000 unique traffic types.

» **Step 2—Count**
Traffic that matches a CLEAR-Flow classifier is counted in hardware. CLEAR-Flow supports up to 112,000 hardware counters that can simultaneously track individual events.

» **Step 3—Threshold**
Constant monitoring of counter values can be implemented with triggers configured to fire as counters exceed pre-determined limits. These limits can be based on counters incrementing too fast, reaching an absolute value, or even based on a ratio between two different traffic counters. Once a threshold is exceeded, administrators have the ability to trigger a predetermined action, or send the traffic for analysis.

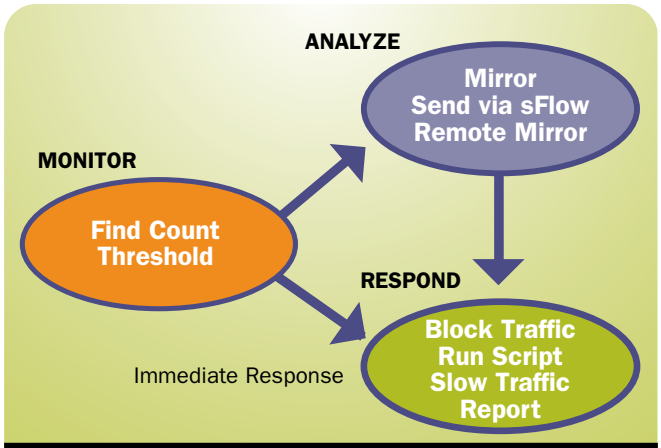



**Figure 2: CLEAR-Flow Process**

## Analyze

Many times the exact nature of a traffic flow is uncertain. In these cases, CLEAR-Flow can send the suspicious traffic to an external device for further analysis. Once the external device has determined the nature of the traffic, better decisions can be made about how to handle the traffic. There are a few different ways that CLEAR-Flow can do this, and specific techniques are more applicable to certain types of network events.

» **Method 1—Mirror**
Copies of the traffic of interest are sent to a mirror port, where a traffic analyzer or intrusion detection system can have complete visibility into the nature of the traffic. Mirrors allow a complete picture of exactly what is happening, and allow for very deep packet inspection.

» **Method 2—Tunnel to Remote Mirror**
This technique is similar to the mirror, except that packets are encapsulated with an additional IP packet header and tunneled off to a remote system for further analysis. For example, this method can be used to send the traffic to a mirror port on a different switch. This allows network analysis equipment to be leveraged over a much larger network infrastructure, as well as enabling better remote debugging.

» **Method 3—sFlow**
sFlow® is a sampling technology that meets the key requirements for a network traffic monitoring solution. Instead of copying the entire traffic flow, using sFlow results in a statistical sampling of the packets being forwarded to a network monitor using the sFlow protocol. This a much more scalable process because a much smaller amount of data is sent to the collector. Using sFlow to report anomalous behavior is most appropriate when it is anticipated that there will be a very high amount of data—for example when monitoring for a DoS attack.

### Respond

Any time a classifier sees a serious threat, a threshold is hit, or an external device draws some conclusion about a traffic flow, CLEAR-Flow allows switches to take action. This allows network administrators to respond appropriately to network events. These actions can include:

» **Option 1—Block the Traffic**
Install an access control list (ACL) entry to completely stop the traffic.

» **Option 2—Run a Script or CLI Command**
Execute a set of CLI commands on the switch. Both approaches allow administrators to run a complex set of commands in response to the traffic.

» **Option 3—Rate Limit**
Install an ACL that slows down the traffic.

» **Option 4—Report**
Send a report to a network management console via an SNMP trap or SYSLOG message.

## CLEAR-Flow Applications for Security

Detecting and reacting to network viruses, worms, and DoS attacks is one of the most difficult problems facing corporate networks today. These attacks are also among the most damaging incidents corporations can face—costing lost productivity or even e-commerce system downtime. CLEAR-Flow can help with both of these problems, adding valuable tools to the network security arsenal.

### Example—Virus and Worm Infection

One of the most pressing requirements for network managers today is the need to identify and quarantine new virus and worm outbreaks as quickly as possible. CLEAR-Flow can provide the critical measurement capability to dramatically shorten the time required to detect and respond to virus events.

In order to accomplish this, CLEAR-Flow filters are configured for each host system on the network to track TCP SYN packets being emitted by each system. This allows CLEAR-Flow to track the number of SYNs being sent by each and every system.

These SYN packets indicate that a system is trying to establish a new TCP connection with a remote system. SYN packets are a normal part of network traffic. However, viruses and worms typically attempt to spread quickly, by opening as many connections to nearby hosts as possible. When this happens, there is a much higher than normal amount of SYN traffic on the network (see Figure 3).

First we count the SYN packets received by the port:

```
entry detect-syn{
if{
TCP-flags SYN;
}then{
count detect-syn
}
}
```

For higher granularity, an individual IP address could also be tracked by adding the source address field:

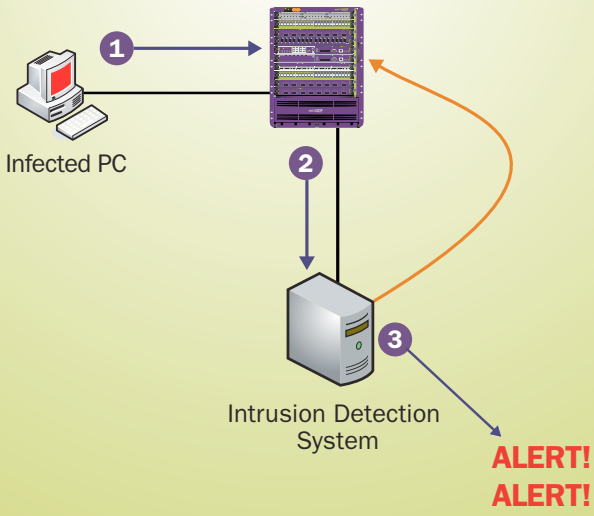
```
entry detect-syn-200{
if{
source-address 10.10.10.200;
TCP-flags SYN;
}then{
count detect-syn-200
}
}
```

Now we create a threshold and specific the action. In this example, we are overriding the global interval and specifying a 5 second interval for the threshold. If the rate of SYNs received is over 1000 for 5 seconds, we will start the mirror.

```
entry eval rate{
 if{
  (rate (detect-syn, 5) > 1000 )
 then{
  sendsnmp 7 "Too many SYNs detected,
starting mirror";
  mirror add detect-syn;
}
```

**Figure 3: Virus and Worm Infection CLI Sample**

If any single desktop system starts to initiate more than a few dozen connections a second, or if a server begins to initiate more than one or two thousand connections a second, then it is highly likely the system is infected with a virus that is attempting to spread itself (See Figure 4). Network administrators may want to immediately block the system from the network, or automatically send this traffic for analysis by the intrusion detection system.




1 Compromised system floods new connections

2 Per-port SYN threshold is hit, switch starts mirroring traffic

3 Intrusion Detection System takes action, blocking source IP address and sending trap to network management

**Figure 4: Detecting Virus Attacks**

## Example—Denial of Service Detection

DoS attacks are a large problem for many companies, especially ones with a significant Web presence. These attacks take down Web sites, e-commerce portals, and other corporate resources. Quickly determining that an attack is happening, and identifying the sources of the attack dramatically reduces its impact.

CLEAR-Flow provides an easy way to detect and respond to DoS attacks. The idea behind these attacks is to overwhelm the server with meaningless messages that tie them up doing busy work, thereby keeping the server from servicing legitimate requests. DoS attacks generally take the form of ICMP ping floods, or TCP SYN floods.

Servers can be protected by adding a CLEAR-Flow classifier for each type of traffic that should be monitored.

If excessive amounts of these types of traffic appear on the switch, CLEAR-Flow will detect the attack, and engage the mirror port or other analysis method. All intrusion detection systems, as well as InMon's sFlow data collector, are capable of detecting the source of these attacks immediately. Once the sources are detected, network operators can block the offenders. This is typically done at the upstream service provider, since these attacks can often consume the bandwidth of the entire connection to the Internet (See Figure 5).

In this example, we monitor traffic headed toward the server farm. One of the types of traffic we will monitor is ICMP traffic.

```
entry icmpcnt{
if{
  destination-address
10.203.134.0/24;
 protocol icmp;
}then{
  count icmpcnt;
 }
}
If more than 100 ICMP packets are
detected per second, block the
traffic.

entry eval rate{
 if{
  (rate(icmpcnt) > 100)
 then{
  sendsnmp 7 "Too Many ICMP packets"'
  deny icmpcnt;
}
```

**Figure 5: Denial of Service Detection CLI Sample**

## Example—Maintaining an Audit Trail

For security conscious environments, it is often desirable to maintain an audit trail for all console traffic traversing the network. Console sessions are often used as a point of attack by hackers, and having an audit log can often be the only way to trace a break-in and prosecute the culprit.

Existing techniques often maintain a log on each server. But hackers have learned to delete such files and to disable these logs in order to hide their tracks after breaching the security of a new system.

Using CLEAR-Flow, simple filters can be enabled to copy all telnet and SNMP management traffic to a mirror port where it can be analyzed and archived as appropriate (See Figure 6).

The hacker won't have any way to know that the network itself is tracing his or her movements, thus making it possible to track the break-ins of even the most sophisticated attackers.

Find telnet packets going toward the servers.

```
entry capture-telnet{
 if{
  destination-address
10.203.134.0/24;
  protocol TCP;
  destination-ort 23;
}then{
 }
}

As soon as we see one,start mirroring
them.

entry eval threshold{
 if{
  (threshold(capture-telnet)>1)
 then{
  mirror add capture-telnet;
 }
```

**Figure 6: Maintaining an Audit Trail CLI Sample**

## Summary

By taking an integrated approach to traffic management, CLEAR-Flow is able to deliver scalable solutions to difficult network problems, while scaling to meet the traffic demands of today's fastest networks. The monitor, analyze, react methodology of CLEAR-Flow creates a very extensible model, which allows users to bring technology to bear on the unique problems of their networks. CLEAR-Flow has many applications beyond those described here, and the number of applications will continue to grow as Extreme Networks continues to add on to CLEAR-Flow functionality.

www.extremenetworks.com

**Corporate and North America**
Extreme Networks, Inc.
3585 Monroe Street
Santa Clara, CA 95051 USA
Phone +1 408 579 2800

**Europe, Middle East, Africa and South America**
Phone +31 30 800 5100

**Asia Pacific**
Phone +65 6836 5437

**Japan**
Phone +81 3 5842 4011


1083_02 02/10