NUS◉FT

No.7

Tech Overview : **An Improvement on Sniffer Mode**

Depending on a business's network management and setup requirements, the Nusoft Internet Recorder can be deployed in either Sniffer mode or Bridge mode.

To deploy the Nusoft Internet Recorder in Sniffer mode, connect the device to the core switch's mirror port. There is no need to make any changes to the topology of the network. Every packet passing through the switch will be duplicated and sent to the Internet Recorder for analysis and recording. The quick and convenient deployment of the device in Sniffer mode makes it a popular choice for businesses.

A proportion of core switch's mirror ports are only capable of duplicating packets out of the port, and will not accept any response packets. In this situation, the IT administrator would not be able to access the Nusoft Internet Recorder's management interface since the switch's mirror port will not accept any response packets. To accommodate to this situation, the device incorporates a "Device Deployment" setting. The IT administrator should select "Sniffer Mode" if Sniffer mode is preferred.

Enabling "Sniffer Mode" on the device will enable the ports to operate as follows:

Port 1 : Act as a receiver of the packets mirrored from the core switch. To prevent packet loops from occurring, the port will not respond to any packets（including ARP）.

Port 2 : Serve for the management of the device. IT administrators can connect to this port to view the device's records. The port can both send and receive packets.

Port 2 for system management
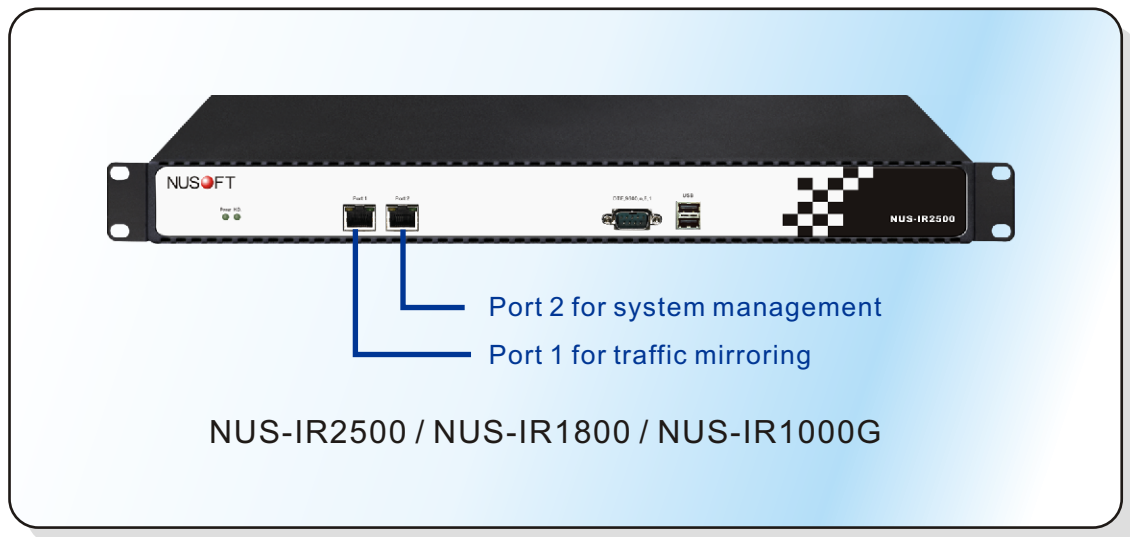Port 1 for traffic mirroring

NUS-IR2500 / NUS-IR1800 / NUS-IR1000G

Figure 1 Sniffer Mode Port Designations for NUS-IR2500, NUS-IR1800 and NUS-IR1000G

To receive data from the company's network for recording, the IT administrator may connect the device's port 1 with the core switch's mirror port. The device's port 2 connects to the company's LAN to provide the IT administrator with access to the device's management interface from anywhere within the LAN.
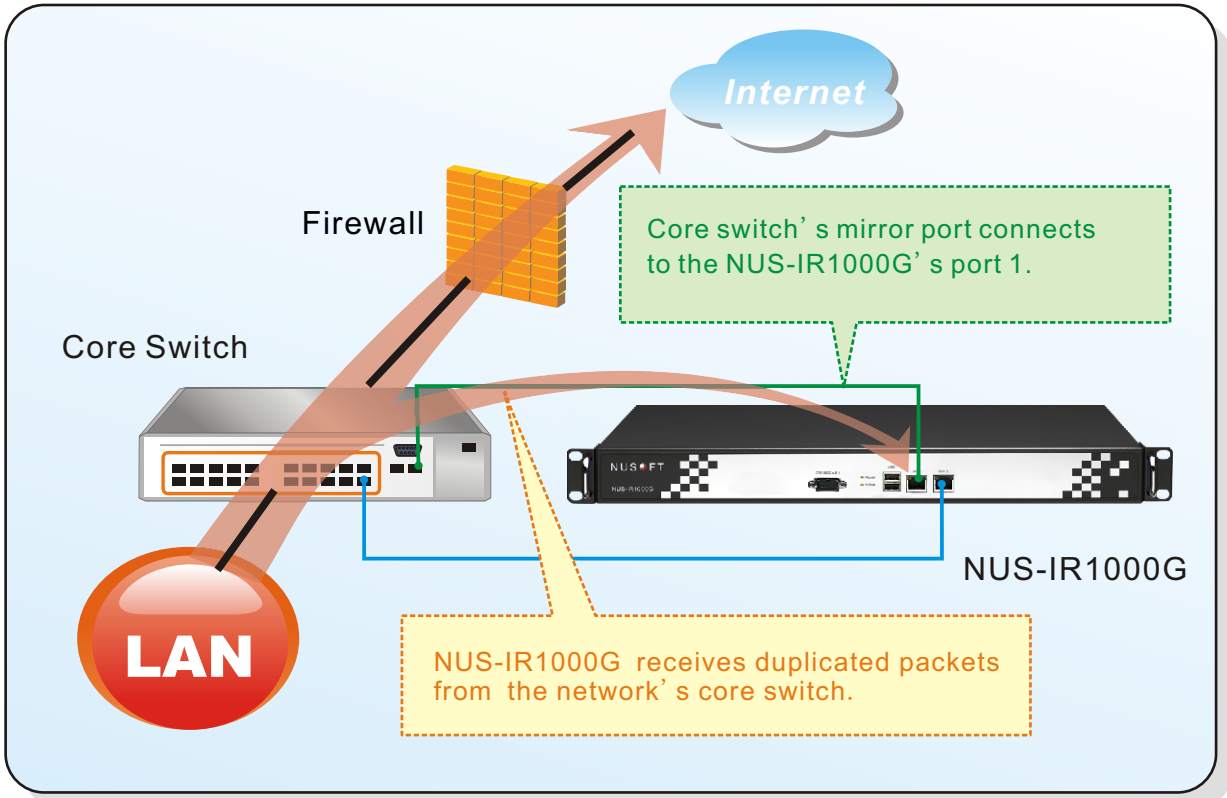
Internet

Firewall

Core Switch

Core switch's mirror port connects to the NUS-IR1000G's port 1.

NUS-IR1000G

LAN

NUS-IR1000G receives duplicated packets from the network's core switch.

Figure 2 The NUS-IR1000G Utilizes the Core Switch's Mirror Port to Capture Data

Internet

Firewall

Core Switch

The NUS-IR1000G's port 2 connects to the LAN

NUS-IR1000G

LAN

The IT administrator accesses the user interface via the port 2
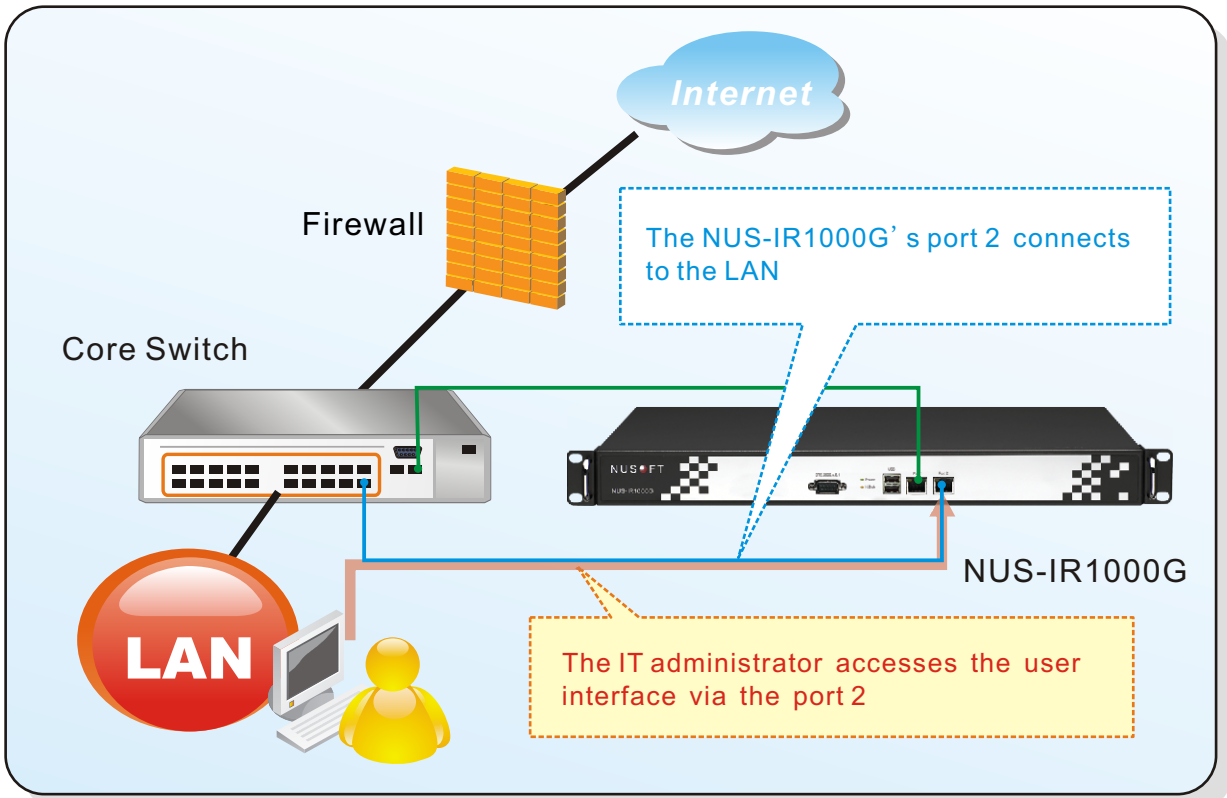
Figure 3 IT Administrator Accesses the Device's User Interface via the Management Port

		Sniffer Mode	Bridge Mode
Deployment Requirements		The port 1 connects to the core switch. The port 2 connects to the LAN.	Install between the firewall and LAN.
Management Controls	Anomaly Flow Detection	Provides alerts but no blocking of the anomaly flow	Provides alerts and can block anomaly flows
	P2P Management	—	Capable
	IM Authentication and Management	—	Capable
Advantages		Suitable if the business doesn't want to alter the setup of their network. Note: This deployment requires a core switch.	The business can fully utilize the device's network management capabilities.

Table 1 Nusoft Internet Recorder's Sniffer and Bridge Mode Comparisons

Product News : Quickly Locate Records via the Extensive Search Features

The Internet benefits businesses in many ways. However, cyberslacking and the leakage of confidential information can cause tremendous harm. To mitigate these problems, businesses all over the world install Internet recording devices from various manufacturers. These devices record vast amounts of data from user's online activities but lack one essential element, namely, an effective manner to locate and view the records.

Even a small-sized business can produce an enormous amount of data for Internet recording devices. Thus, IT administrators need an efficient way of locating the desired records and an effective method of reading the data. In response to this, Nusoft's Internet Recorder series has addressed this issue.

Taking the NUS-IR2500 as an example, the device accurately records users' online activities by details of each service, e. g. , username, IP address, time, etc. (It varies with services.) The IT administrator can conveniently gain access to these data at any time in the future.

SMTP / POP3 Email Search
Compared to third-party Internet recording devices, the NUS-IR2500 in addition to merely searching by sender, recipient, subject, time, etc. also features attachment and content searching.

Web-Based Email Search
Third-party Internet recording devices are incapable of determining the sender, receiver, subject, etc. since they only capture screenshots of web-based emails. Thus, the only criterion they can search by is email service provider. The NUS-IR2500's search engine performs web-based email searches in a similar convenient and comprehensive fashion to ordinary email.

HTTP Web Page Search
The NUS-IR2500 is now capable of conveniently searching web sites based on the URL or content to locate the desired web page. Other third-party recorders are only capable of narrowing down search results based on the date.

Instant Messaging Search
The device is capable of locating recorded conversations based on a number of criteria such as username, IM account, participant, content, etc. In addition, instant messaging file transfers can also be searched.

FTP Search
For IT administrators to quickly locate the desired FTP records, they need a complete range of search criteria, which is what the device provides. Search criteria include file name, hostname, username, IP address, file size, session direction, date, etc.

Telnet / BBS Search
The device provides search criteria such as the hostname, session direction, etc. allowing the IT administrator to locate the desired record efficiently.

IP Service	Searchable Criteria	
	Nusoft Internet Recorder	Third-Party Internet Recording Devices
Email (SMTP, POP3)	Recipient, sender, subject, content, username, IP address, session direction, with/without attachment(s), attachment name, session direction and date	Recipient, sender, subject, username and date
Web-based Email	Recipient, sender, subject, content, username, IP address, session direction, with/without attachment(s), attachment name, session direction and date	Username, URL, email service provider and date
HTTP Web Page	URL, username, IP address, website content, session direction, file transfer (upload / download) and date	Date
Instant Messaging	IM application, session direction, IP address, username, IM account, participant, conversation content, transferred file name, authentication name and date	Username, IM account, participant and date
FTP File Transfer	File name, hostname, username, IP address, file size, session direction and date	File name, IP address, username, account, session direction and date
Telnet / BBS Session	Username, IP address, hostname, session direction and date	Username and date

Table 2 Comparisons with Third-Party Internet Recording Devices by Search Feature