Tech Overview : Effective Storage Space Management

Internet recording devices are an essential part of any business' s network. If confidential business information and cyberslacking are not kept under control, the consequences can be costly. To be effective, these devices need to incorporate accurate and detailed traffic flow analysis with network management and easy-to-interpret statistical reporting.

Storage space is an important factor for these devices, as the records from recording various activities across the entire network that each user amasses. Large in built storage capacities can be good for the short term, but in the long term, they will eventually reach its capacity. Storage capacity management is required to resolve this issue.

Nusoft' s Internet Recorder series bases storage space allocation on the service e.g. HTTP, instant messaging, etc. Depending on each service' s degree of importance, the maximum required storage time can be individually configured. For example, HTTP can be set a shorter time compared to services of greater importance such as instant messaging and email (SMTP, POP3, Web SMTP and Web POP3), ensuring that storage space is used efficiently.

During normal operation, the Nusoft Internet Recorder' s inbuilt hard disk either keeps records for each service based upon the "Storage Time" setting when reaching its capacity or deletes records chronologically starting from the oldest ones.

1. The built-in hard disk has not yet reached its storage capacity

Each service such as SMTP, POP3/IMAP, HTTP, IM, Web SMTP, Web POP3, FTP and Telnet is individually allocated storage space by the Nusoft Internet Recorder. Depending on the needs of the business, the amount of days to keep each service' s data can be individually set to ensure efficient use of the available storage space.

As an example, if SMTP is set a maximum storage time of 30 days. Any data recorded on January 1st will be will be automatically deleted by the device on January 31st.

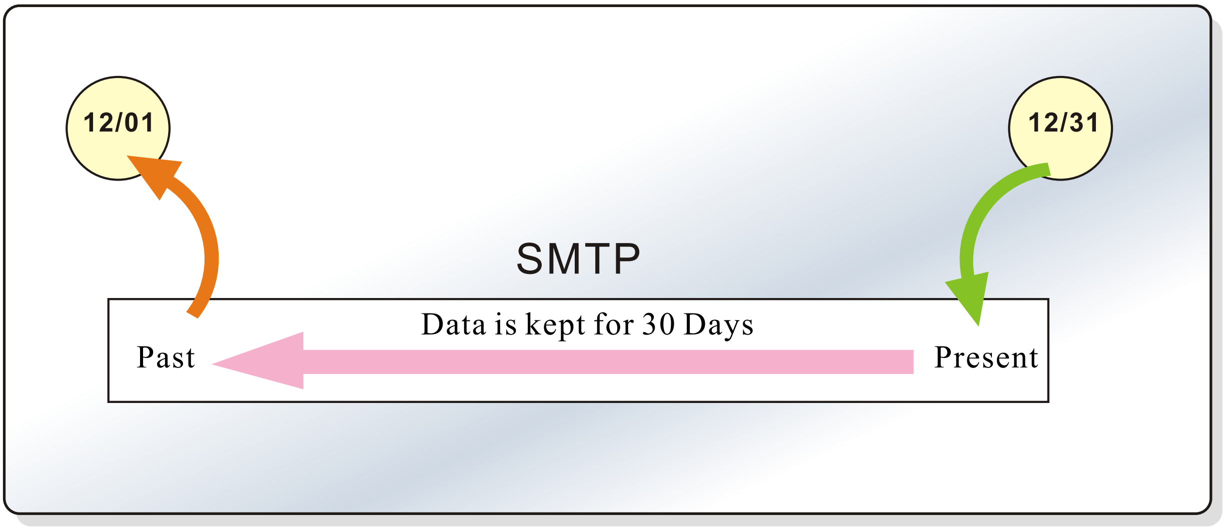

Figure 1 Deletion of Data Based on Storage Time

2. The built-in hard disk storage usage has reached full capacity

The second situation occurs when each service has not yet reached its maximum storage time, but the device has reached its storage capacity. The device will delete records chronologically beginning from the oldest records first.

When the inbuilt hard disk has not yet reached its storage capacity, data is deleted according to each service' s storage time setting. However, when it has reached its capacity, old data will be deleted to provide space for the new data. For example, if the device begins to records 10MB of new SMTP data, 10MB of old data will be deleted to free up space for the new 10MB records.

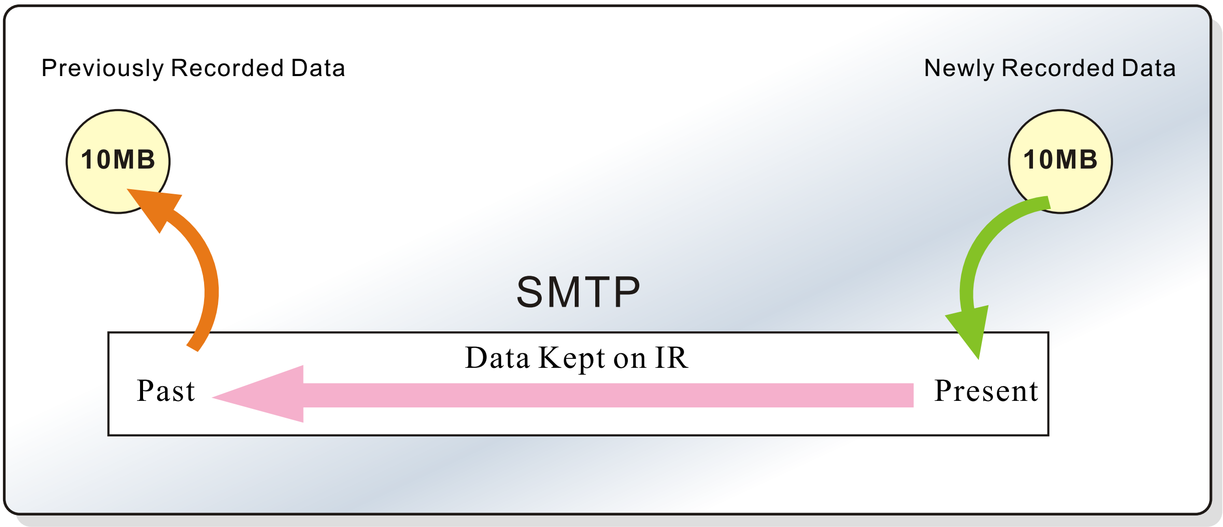

Figure 2 Storage Space Allocation

- **Remote Backup**

To satisfy various laws around the world requiring the archiving of data such as email for a period of years, and to prevent the loss of emails due to accidental deletions, the device offers a Remote Backup function. Data can be backed up to a file server, NAS, Samba server or other NetBIOS capable storage device, to provide a potentially unlimited storage time and space.

Product News : Preventing Viruses through Instant Messaging Management

The Internet is an endless source for viruses of various forms. Not only can they cause major disruptions and the loss of data, but they also contain the potential to steal sensitive business information and personal data.

The widespread use of instant messaging software has attracted the attention of hackers and virus writers. Malicious programs such Internet bots, can utilize instant messaging software to obtain files and confidential information from the PC or internal networks that they are attached to. They are spread through security flaws in the instant messaging software or simply by a click on a vicious link.

IT administrators are left with determining the best form of action to take against these malicious programs.However, the most effective way of dealing with this issue is to manage the use of instant messaging software to ensure that viruses cannot be spread.

For large enterprises containing many users, different management policies might need to be applied to specific individuals or groups. For example, some departments might have no need to use the software, whereas other departments might need it to communicate with clients.Therefore, in most situations it is inappropriate to ban its use across the entire organization.

Nusoft Internet Recorder provides the ideal solution to this problem. It provides detailed and accurate records of conversations. It supports a large number of commonly used instant messaging software（including web-based instant messengers）. Specific users can be permitted or denied IM login, using controls from the device such as authentication. They can also be permitted and denied the use of encrypted instant messages and the transmission of files. Signature definition files allow the device to continue managing instant messaging software effectively.

In order for a company to take full control over their employees' instant messenger use, the device's group management capabilities allows different management policies to be applied to an individual user or entire group.

- **Supported Instant Messaging Software:**

Supported Items		
Conversation Recording	**Login Blocking**	**File Transfer Blocking**
MSN	MSN	MSN
Yahoo Messenger	Yahoo Messenger	Yahoo Messenger
QQ	QQ	QQ
ICQ	ICQ	ICQ
AIM	AIM	AIM
Gadu-Gadu	Gadu-Gadu	Gadu-Gadu
Skype	Skype	Google Talk
Official MSN Web Messenger	Google Talk	

Table 1 Supported IM Software and Controls

- **Supported Web-Based Instant Messengers**:

Official MSN Web Messenger, Buddy, ILoveIM, Meebo, IMhaha, KoolIM, MessengerFX, Communication Tube, IMUnitive, Goowy, MSN2Go, ToToMoMo, Mabber, Wablet, Mobile, Web QQ, etc.

IM Software Management Capability	MSN	Yahoo	QQ	ICQ/AIM	Skype	Gadu-Gadu	Google Talk
Permit users to send unencrypted messages only	✓	–	–	–	–	✓	–
Permit only authenticated users to send unencrypted messages	✓	–	–	–	–	✓	–
Permit only authenticated users	✓	✓	✓	✓	–	✓	–
Permit all users	✓	✓	✓	✓	✓	✓	✓
Block all users	✓	✓	✓	✓	✓	✓	✓
Permit only users with a valid password	–	–	✓	–	–	–	–
Permit only authenticated users with a valid password	–	–	✓	–	–	–	–
Permit only users who have installed the IR plug-in	–	–	–	–	✓	–	–
Permit users using official Web IM	✓	–	–	–	–	–	–
Permit users using Web IM	✓	✓	✓	✓	–	–	–
Block users using Web IM	✓	✓	✓	✓	–	–	–
Block IM file transfers (note: the device must be deployed in Bridge mode)	✓	✓	✓	✓	–	✓	✓

Table 2 Supported IM Software Management Capabilities