LINKSYS®
A Division of Cisco Systems, Inc.

Connected Office Business Organization
Solutions Engineering

White Paper:
Network Storage for the Small Business

EDCS-593805 v1.0

Corporate Headquarters
Linksys, a Division of Cisco
121 Theory
Irvine, CA 92617-3045
USA
http://www.linksys.com
Tel: (800) 546-5797
(800) 326-7114 (Technical Support)
Fax: (949) 823-3007

Contents

Introduction

The need for shared storage is becoming a lot more prevalent than in the past. A storage solution can affect many different aspects of the business including revenue and profitability, growth and expansion rates, employee and IT staff productivity, customer experience and satisfaction and capital and operating expenses. A major challenge for today's business is how to manage storage growth while ensuring data availability and business continuance.

Storing and backing up important data typically requires more than a consumer storage solution. Yet a major challenge for storage deployments is the complexity that arises from provisioning, maintaining, and managing complex storage environments. Different applications have varying storage needs, and this has resulted in the proliferation of multiple, independent types of data storage. The associated capital and operational costs can strain administrative staff and IT budgets.

This white paper discusses the unique benefits that Linksys brings to network attached storage (NAS) solutions. It also provides a solution architecture based on Linksys Network Storage System (NSS) for a business to store, backup, share and archive critical company or customer information on an on-going basis.

Audience

This publication is intended to provide guidance to Linksys customers, Value Added Resellers (VARs), Linksys network design engineers and network managers.

Scope

This white paper provides network storage solutions for a Small- to Medium-sized business (SMB) with less than 100 employees, and uses an example set of products from the Linksys Business Series family. The storage concepts and their underlying technologies covered in the paper are as follows:

- NAS Storage Consolidation and Virtualization
- RAID (Redundant Array of Independent Disks) controller
- Security
- Backup & Restore
- Performance

Related Documents

[1] Linksys Connected Office Reference Network Architecture [EDCS-579560 V1.0]
[2] Business Series Network Storage Systems Product Brief
[3] Linksys Approved Vendor List (AVL) For Network Storage Systems

Networked Storage Overview

Many small businesses are looking to leverage advanced database technology to power a range of e-business and on-demand business applications. This range of applications is driving tremendous demand for storage capacity and information management, straining networking resources and IT budgets within the small business environment.

Linksys is ideally positioned to address these challenges with a line of business grade Network Storage Systems (NSS) that bring a robust Network Attached Storage (NAS) solution within reach of today's budget minded businesses. The Linksys NSS is specifically designed to offer businesses easy to use, flexible, cost-effective storage solutions that keep pace with business growth and that reduce the total cost of doing business.

Storage Solution

The key design consideration for a storage solution is that it should accommodate the business' applications. The application and data management needs of most SMB IT environments are typically served by a NAS approach. Accordingly, the storage architecture in this white paper describes a NAS storage solution.

The reference NAS solution architecture enables (Figure 1):

- Secure data sharing in a LAN environment with storage centralization
- Virtualization across multiple NSS devices; and
- Secure remote storage backup options for "offsite" backups

These capabilities enable the business to deploy a more scalable, reliable storage solution and backup environment at lower cost.

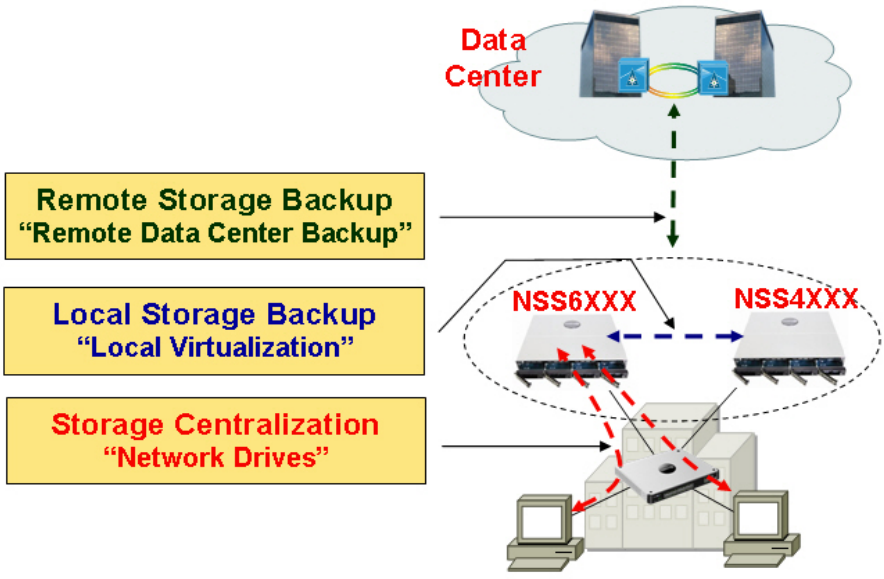

Figure 1: NAS Topology

Linksys NSS are NAS appliances that are dedicated to disk-based storage and attach to the user LAN through an ordinary network connection. Storage can be aggregated as volumes or as "virtualized" sets over multiple local NSS devices. Virtualization is the ability to export disks or RAID sets from 'secondary' NSS devices that are in your network and import them to a 'master' NSS device. Virtualization reduces downtime and optimizes storage utilization.

The reference storage solution architecture is illustrated in Figure 2:

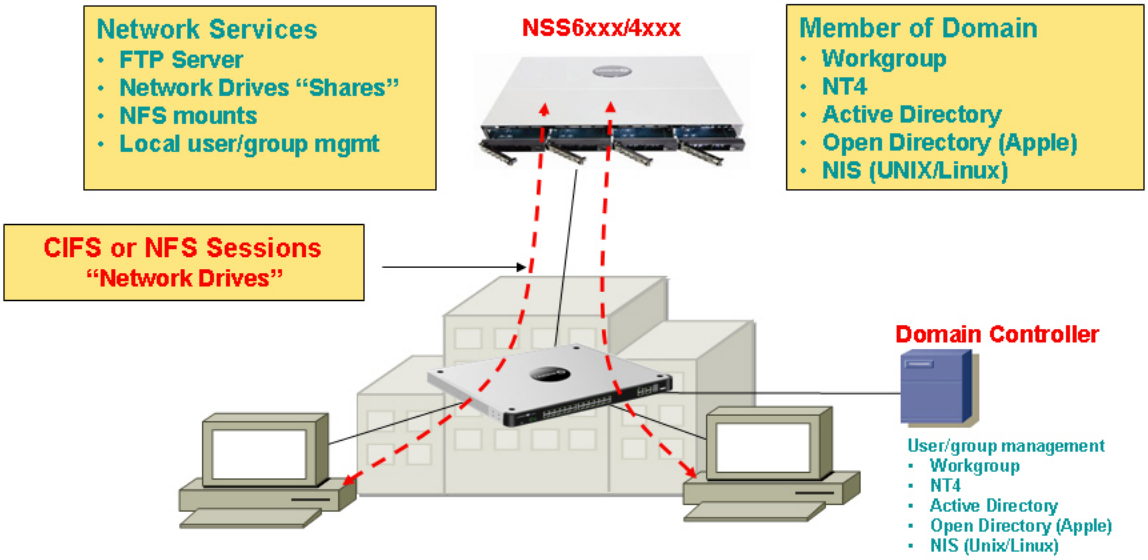

Figure 2: Storage Solution Reference Architecture

In Figure 2, the Linksys NSS appears as a native file server for clients within the network. Cross-platform file systems are supported including: Windows, Apple Macintosh, UNIX and Linux. Files retain their native file format when stored on the NSS.

File servers sit on the LAN and are connected to the NSS by a standard Ethernet network. Client systems use standard file access protocols such as CIFS (Common Internet File System) or NFS (Network File System) to make storage requests. Functionally, CIFS or NFS file system 'shares' appear as folders within the corresponding system directory. Users typically map a NSS as a network drive on their PC, or access it via FTP. Multiple users on disparate systems can access data simultaneously. Logically, the drives appear to be directly attached their own computer. On the Windows or Linux system the NSS will appear as another disk drive or mount point.

Local file system calls from the clients are redirected to the NSS device, which provides shared file storage for all clients. If the clients are server systems, the NSS offloads the data management overhead from the servers. If the clients are desktop systems, the NSS provides "serverless" file serving.

Volumes are used to partition the space that is available on an NSS array set as follows:

- On-disk data encryption is either enabled or disabled for each volume when it is created.
- Existing volumes can be expanded, but not contracted.
- Each volume contains one or more shares, which logically subdivide the volume, such that users using one share cannot see files that belong to another share.
- One volume must be assigned at initial system configuration as the Home Directory Location (the volume that contains the home directory for all user profiles).

The typical organization will assign users a profile which defines the groups to which they belong. Shares define the access to a volume: group and user level read and write permissions and which protocols (CIFS, NFS, FTP, DFS) are supported (Figure 3).

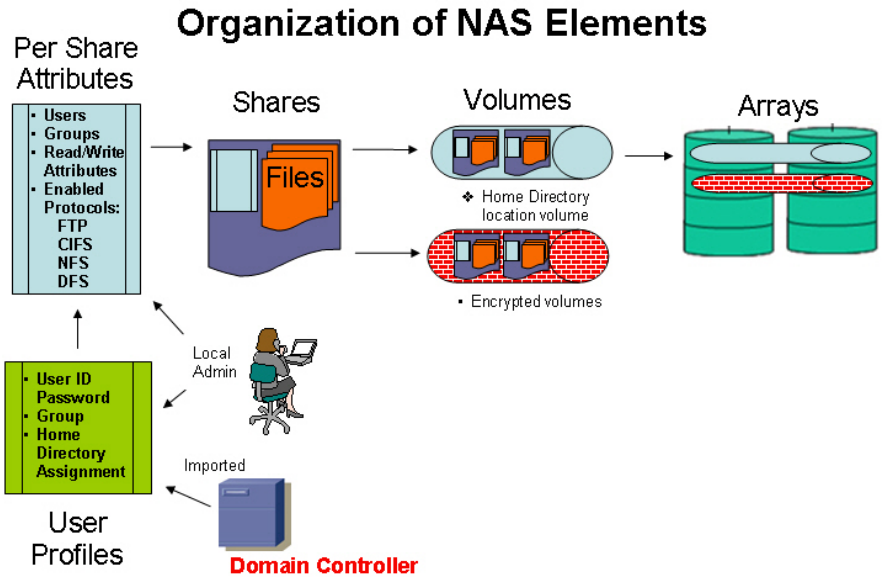

Figure 3: Organization of NAS Elements

Each NSS operates as a LAN attached device within the network infrastructure. Unless it is strictly being used as an FTP server, the NSS is required to be enabled as a component within your Windows, Apple Macintosh and/or Unix/Linux system directory (e.g. Microsoft's NTv4 Domain, Active Directory, Apple's OPEN Directory, Network Information System (NIS) Domain for UNIX and Linux platforms) such that users can create CIFS or NSF connections to the NSS from their PCs. Each user connection counts one against the concurrent user maximum for the NSS.[1] User and group membership is typically managed on the domain controller for the system directory (NTv4, Active Directory, OPEN, NIS). User and group definitions (and share access) that are local to the NSS may be defined.

A VAR or end user can purchase the NSS device and directly connect it to any network switch in the customer premise that supports 10/100/1000 Ethernet. The NSS device is configured to automatically obtain an IP address (DHCP) out of the box and is managed via a secure web-based management GUI. A simple utility called NASDiscovery.exe is available to allow the administrator to connect a PC on the same LAN segment as the NSS device. The utility also enables the administrator to determine the current IP configuration for the NSS and to perform the initial configuration. The NSS device is accessible remotely via the secure web-based GUI. Users who have access to their corporate intranet can access the NSS device at any time.

Network storage as you will see is achieved not by a single technology or tool, but a culmination of technologies working together as part of an overall solution. The following sections walk through these technologies and describe how they are used to address business efficiency and availability requirements.

[1] See Linksys NSS4000/NSS6000 product data sheets for specific device maximums.

Storage Concepts and Technologies

Network Attached Storage (NAS)

The term network-attached storage (NAS) refers to a storage device that is connected to a network (usually TCP/IP) and provides remote file access service. The end hosts access the files stored on the NAS device using common file access protocols such as NFS or CISF. To an end host, a NAS device appears as a NFS or a Windows file server.

A NAS device is a collection of multiple physical disk drives organized into one or more logical (potentially redundant) storage units or RAID (Redundant Array of Independent Disks) arrays that perform as network accessible storage on the LAN.

While direct-attached storage (DAS) works well in environments with an individual server or a limited number of servers, the situation becomes unmanageable if there are dozens of servers or significant data growth. Storage for each server must be managed separately and cannot be shared with DAS. Performance and scalability are often limited, and storage resources cannot be efficiently allocated.

NAS is the most mature networked storage solution, and the type of networked storage that allows data sharing by connected host systems. The advantage is that everyone on the network can store files on the NAS system. Linksys NSS is a NAS system that delivers several other 'business-grade' advantages, including improved scalability, reliability, availability, and performance. The Linksys NSS device consists of an engine that implements remote file services (NFS/CISF server) and manages all the drives on which data is stored.

LAN Infrastructure

Because throughput for a NAS system is gated by the disk read/write performance, a single active Gigabit Ethernet link typically provides sufficient throughput capacity to address most business requirements. However, heavy data transfers can overwhelm a LAN if multiple systems are in use. You should understand the implications of LAN traffic on the intended network segment, and plan to accommodate upgrades or network infrastructure changes that might be needed to achieve best performance.

The recommended LAN infrastructure for a storage solution is to enable redundant connections to the network so that there is no single point of failure (Figure 4):

- Connect the ports to different switches and
- Set the configuration on the NSS for "primary and backup" link operation.

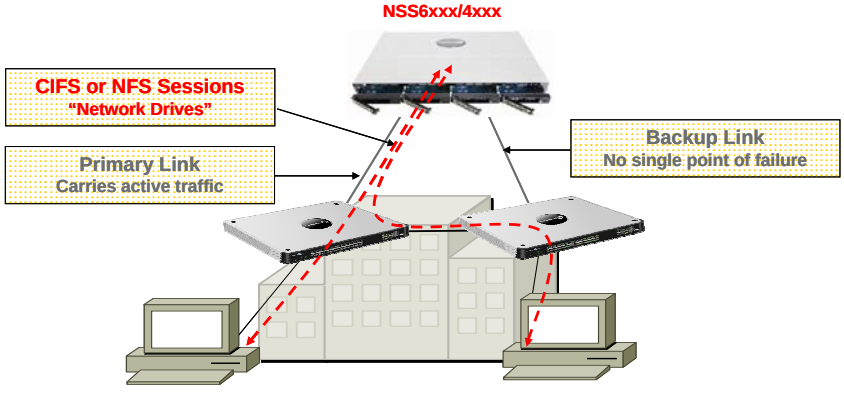

Figure 4: Redundant Network Attachment

Alternatively, the ports may be configured as a single logical link (aggregation) to a single switch (Figure 5).

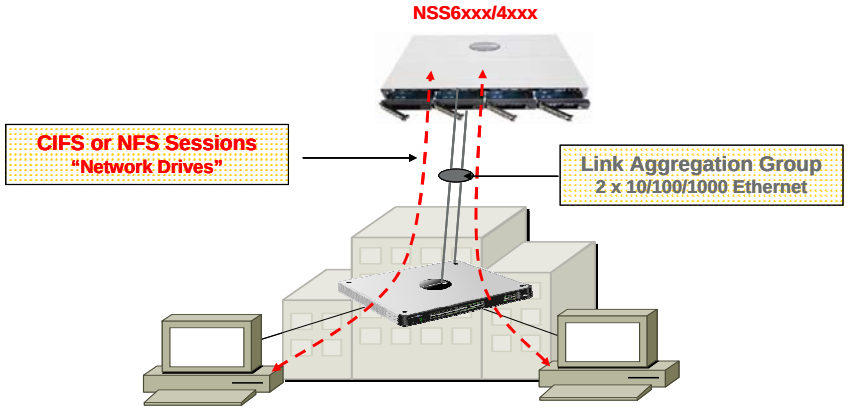

Figure 5: Link Aggregation

Each NAS device should provide Ethernet connectivity with enough ports to support the expected storage traffic. For example, the Linksys NSS supports two redundant Gigabit Ethernet (10/100/1000Mb Ethernet) links for connectivity. The NSS also supports advanced LAN functions with VLAN mapping and tagging, QoS control and link aggregation.

Storage Centralization/Aggregation

The business can defer large investments in storage with storage centralization or aggregation. Rather than the total volume of storage being fragmented across multiple devices, network drives are consolidated into a dedicated storage infrastructure that allows much greater levels of utilization to be achieved. Storage can be bought and deployed on a "just-in-time-storage" basis and provisioned on an as needed basis. Tasks like backup can be done once for the consolidated storage system, rather than for multiple independent systems. Storage aggregation is supported across the family of Linksys NSS products.

Storage Virtualization

Virtualization is about scaling storage capacity while simplifying user access via a single virtual system. Virtualization can be utilized when there are two (2) or more NSS devices located at the premise. Virtualization allows volumes that are physically located on "Slave" NSS units to be logically assigned to a local "Master" NSS system (NSS6000). The virtualized storage appears as a single logical storage unit on the Master, allowing volumes and shares to span the entire storage array.

Up to 4 disk sets may be imported per master NSS device, where they are combined to create a JBOD (Just a Bunch Of Disks) set. This JBOD appears to the users as one large unit of disk space on the network, upon which volumes and user shares are then created. This allows the users to access all storage for that virtualized system via a single network drive location.

Design consideration should be given to the RAID levels that are used in virtual sets. It may be beneficial to enable a JBOD that is entirely constructed of RAID 5 sets or RAID 10 sets. This approach ensures that all the capacity within the JBOD performs to the same redundancy and fault-tolerance capabilities. In the example below (Figure 6), two (2) striped RAID sets are exported from the outside NSSs (a NSS6000 and a NSS4000) and imported on to an NSS6000, such that the master system presents two array sets to the user: 1) a JBOD set (containing both imported Striped arrays); and 2) a RAID mirror set.

Administrators assign shares to each set based upon user requirements for either Striped or Mirrored protection.

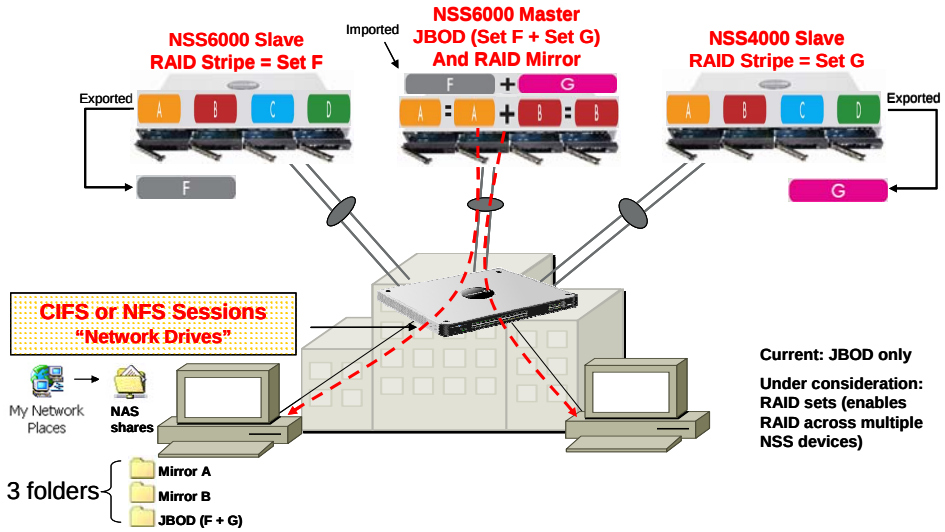

Figure 6: Virtualized Storage

Note

Virtualization can be done with both the NSS6000 and NSS4000. However, a virtualization master may only be an NSS6000 series. A slave may be an NSS4000 or NSS6000.

Distributed File System

While virtualization can assist the administrator in managing storage capacity, Microsoft Distributed File System (DFS) is designed to make it easier for Windows users to find files when storage is defined on multiple volumes. DFS provides access via a single set of shares with a unified hierarchy, rather than defining one share per volume (Figure 7). DFS support is enabled/disabled on a per share basis.

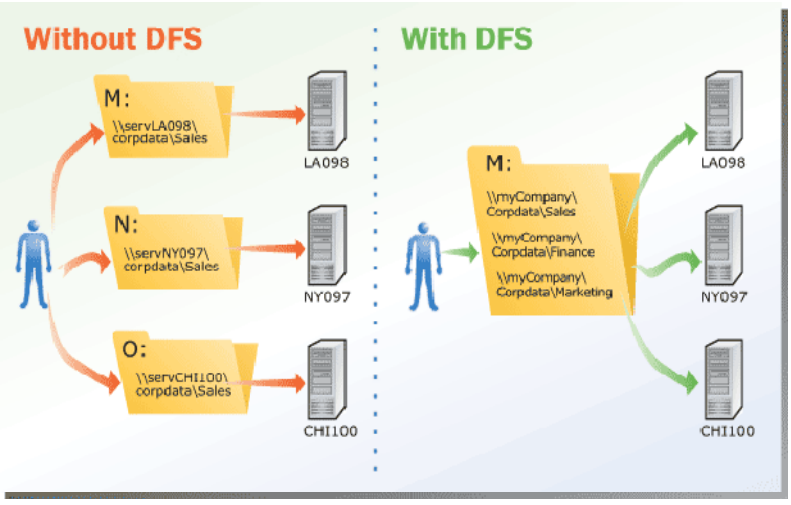

Figure 7: Distributed File System (DFS)

RAID

RAID (Redundant Array of Inexpensive or Independent Disks) is a method employed in a network for using multiple hard drives (in a storage array) to improve performance and/or reliability in information storage. Your choice of RAID will impact both the reliability and the total usable storage capacity of the NAS appliance.

There are various RAID levels (or ways to define how the disks work together) that provide one or more of the following benefits:

- Increased data integrity
- Fault-tolerance
- Improved Read and/or Write throughput or capacity

Consider the RAID levels that will be most beneficial for the business. Linksys NSS products offer data protection through internal RAID. NSS devices support RAID Levels: 0, 1, 1+Spare, 5, 5+Spare, 10, and JBOD. You can configure the NSS boxes to have two (2) independent disk RAID Arrays (e.g. RAID0/1/JBOD).

Note

From an end-user perspective, the RAID array appears as a single data repository instead of multiple individual hard drives. Administrators may assign multiple volumes with different levels of accessibility to the array.

RAID types should be carefully chosen according to business resiliency requirements. The decision is generally based upon a trade-off between expense and features (e.g. performance, fault-tolerance and data integrity), and the applications for which the array is storing information. While there is no single correct RAID level for any application, some basic design considerations may be helpful:

- Some type of data integrity/fault-tolerance is generally desired. This requires that one of the parity or mirroring RAID types should be considered. For example, RAID 1 creates two complete copies of your data. Disk drives are very reliable devices, but they do fail. Having two complete copies of data ensures that the business continues with minimal disruption.
- Applications with real-time requirements, such as video surveillance and database lookup, may benefit from RAID types with improved disk read and disk write performance that are generally found in striping solutions. As such, RAID 5 and RAID 10 configurations should be among those considered.
- RAID 0 is not for business use, unless your business is video editing or an environment where you always keep a copy of your data in a safe place, and you need the very highest performance and your file sizes are large.

Note

In their default configuration (out of the box), NSS4100 and NSS6100 systems include a RAID 5 configuration across four (4) 250GB drives.

Virtualization, which allows multiple RAID sets to be exported to a master NSS, can be used to aggregate multiple fault-tolerant RAID sets into a single JBOD architecture. This can simplify user operations by allowing all users to access a single "virtual" set, while enabling a scalable and fault-tolerant architecture to be deployed.

The number of RAID level implementations is continuously changing as new methods and combinations of methods are developed and the technologies continue to improve. The following sections provide a brief overview of the RAID levels supported by the Linksys NSS series of NAS and their advantages and disadvantages.

RAID 0 (Striped Set)

RAID 0 splits data evenly across two or more disks. Data is written in blocks across multiple disks. Because it contains no parity information, it offers no redundancy. Because the data is striped across all the disks in the array, the reliability of a given RAID 0 array is equal to the average reliability of each disk divided by the number of disks in the array. For example, a set of two disks is roughly half as reliable as a single disk (Figure 8). RAID 0 is useful where redundancy is not a requirement. The following design considerations apply:

- This RAID level should not be used for mission-critical systems.
- Minimum Number of Disks: 2
- Advantages: High performance. All storage on the disks is usable.
- Disadvantage: No fault tolerance. If one drive fails, the entire array becomes inaccessible.

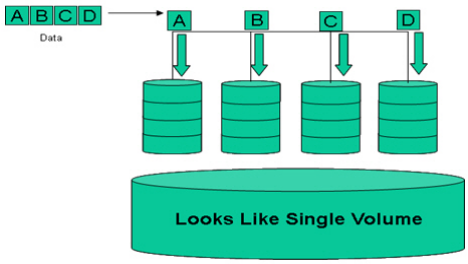

Figure 8: RAID 0

Note

When you stripe disks of different sizes together, the storage space added to the array is no larger than that of the smallest disk in the array. For example, if you put three disks of sizes 100 GB, 120 GB, and 120 GB into the array, the total storage space of the array is 300 GB.

RAID 1 (Mirror)

RAID 1 provides data redundancy by writing data to one, two or three other hard disk drives in the array. The mirrored disks have 2x, 3x or 4x the Read transaction rate of a single disk and the same Write transaction rate and transfer rate per block as a single disk (Figure 9). The following design considerations apply:

- Use this RAID level for systems where high-availability is critical.
- Minimum Number of Disks: 2
- Advantages: Best data protection of the RAID levels as it is 100% redundant.
- Disadvantages: Highest disk overhead (i.e., 100%) of the RAID levels. For example, if there are two 80 GB disks, with a total of 160 GB of raw space, the amount of protected space equals 80 GB.

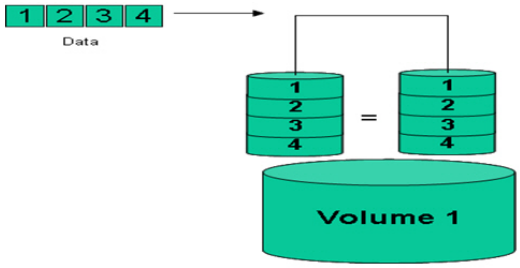

Figure 9: RAID 1

RAID 1+Spare (Mirror + Spare)

Select RAID1 + Spare to dedicate another disk as the automatic backup when one member of the mirrored configuration fails. This ensures that if a disk fails a spare disk is available to automatically replace the failed disk (Figure 10). The following design considerations apply:

- Minimum Number of Disks: 3
- Advantages: Excellent redundancy. Good performance.
- Disadvantages: Costly.

The spare disk is not used until a working disk fails. For example, in a two-disk mirror where each disk is 80 GB, the total raw space is 160 GB, of which 80 GB is protected and 80 GB is available for use. There is also 80 GB of space available. This means that of the 240 GB of total space, only 80 GB is actually usable at any given time.

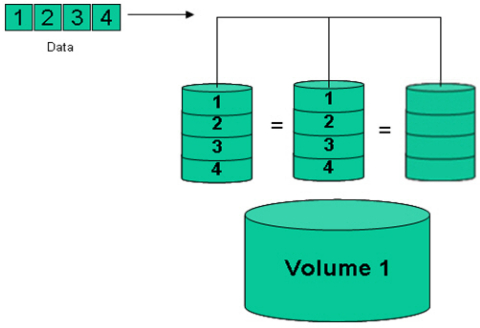

Figure 10: RAID 1+Spare

RAID 5 (Striped + Parity)

RAID 5 is one of the more popular and versatile levels implemented due to its excellent performance (that is, high Read transaction rate, medium Write transaction rate, and low ratio of parity disks to data disks) and good fault tolerance. It uses block-level striping with parity data distributed across the disks in the array. This means that every time a block is written to a disk in the array, a parity block is generated within the same stripe.

RAID 5 stores parity data which can be used to rebuild data should data become lost or corrupted, but not full redundant data. The calculated value is stored on each disk on blocks allocated to parity. This means that the amount of usable space for the protected disk is decreased due to the parity space requirements. The amount of available protected space is decreased by the size of the single disk. For example, if there are three 80 GB disks in the array with a total of 240 GB of space configured as RAID 5, the usable space equals 240 minus 80 which equals 160 GB of protected usable space. If one of the drives fails, the missing information can be recreated using parity bits stored on the remaining members. Use this RAID level for applications such as Intranet servers; database servers; Web, e-mail, and News servers; and File and Application servers (Figure 11).

The following design considerations apply:

- Minimum Number of Disks: 3
- Advantages: Good balance between space usage and disk protection. Higher read performance than RAID1; similar to RAID 0.
- Disadvantages: Because of the parity that must be calculated, write transactions are somewhat slower than read transactions. It is resource-intensive to rebuild in the event of a disk failure (as compared with RAID 1).

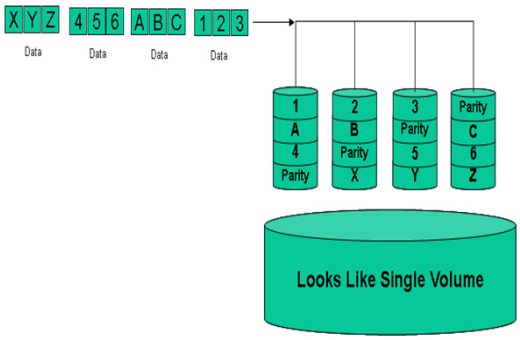

Figure 11: RAID 5

RAID 5+Spare (Parity + Spare)

The RAID 5 + Spare configuration adds a "hot spare" to RAID 5 (Figure 12). The following design considerations apply:

- Minimum Number of Disks: 4
- Advantages: This option increases the overall system reliability so that when a disk fails within the array, the spare can be used to rebuild the data existing on the failed disk. Sparing helps to minimize the time before a disk rebuild begins, so it minimizes the time that the system is vulnerable to additional drive failure.

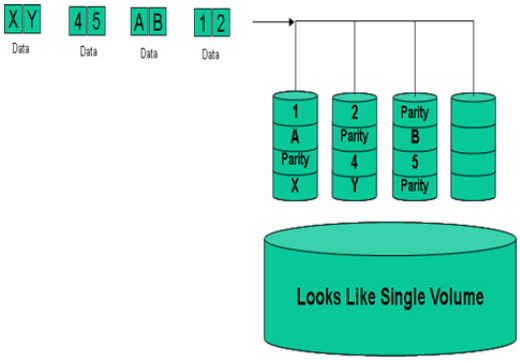

Figure 12: RAID 5+Spare

RAID 10 (Mirror Then Stripe)

This RAID level has multiple variations but can be thought of as a two-layer hierarchy of RAID levels. Two or more RAID1 arrays form the lowest level and are then striped to form a RAID0 array. The following design considerations apply:

- Minimum Number of Disks: 4
- Advantages: This level provides a high degree of redundancy and can be used for databases with high loads due to its faster write speeds than those levels that use parity for calculations. It also increases the overall system reliability so that when a drive within the array fails, the spare can be used to rebuild the data existing on the failed drive.
- Disadvantages: Expensive. All disks must move in parallel with proper track lowering sustained performance. Limited scalability given high cost.

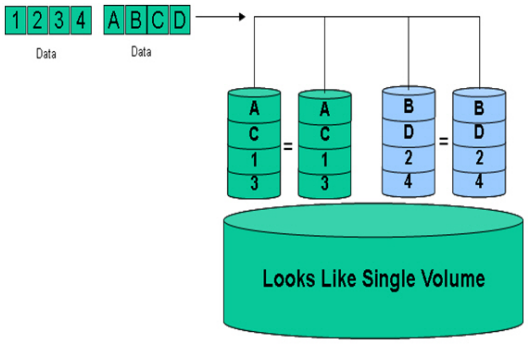

Figure 13: RAID 10

JBOD – (Linear) - (Just a Bunch of Disks)

JBOD is technically not one of the numbered RAID levels. It provides a way to group a set of physical disks together to appear to the operating system as a single disk (Figure 14). With a JBOD, you can concatenate disks of varying sizes into one logical unit. For example, one drive could be 3 GB, one 15 GB, one 5.5 GB to make a logical drive of 23.5 GB. The following design considerations apply:

- Advantages: Disks of varied sizes can form a single logical unit. Unlike RAID 0, if a single drive fails in a JBOD, only the data on the affected drive is lost. In a RAID 0, this usually means the loss of all the data in the array.
- Disadvantages: There are no performance benefits and there is no data protection.

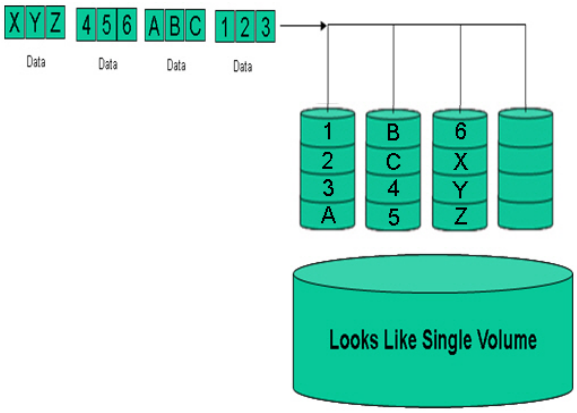

Figure 14: JBOD

Storage Security

Storage networks have traditionally been considered "secure" because deployments have been limited to a subset of a single data center on an isolated network. This perception is changing with the reach of storage networks over the Internet. It is becoming more common to read about information assets (sensitive proprietary data, credit card information, etc.) being compromised via unauthorized storage access. Unlike other storage vendors, Cisco and Linksys have a legacy of securing networks for our customers. Linksys is uniquely qualified to help protect precious information from both externally and internally launched attacks with the following capabilities that are built into Linksys NSS products.

Access Control

NSS secure access control allows the business to limit or allow access to the NSS and volumes on an as needed basis. Access to the system in general is controlled by user ID and password authentication, generally in conjunction with a directory service (as described

previously). Users must have an ID on the system in order to open a CIFS, NFS or FTP connection.

Data privacy is provided by the partitioning of volumes into shares as follows:

- Users and groups must have been granted access to a share in order to see files on that share.
- Within a share, access is controlled by the group and user read/write permissions, defaults for which are defined for each share contained on a volume.
- Each user is assigned a profile (either provided by a system directory or defined locally on the system) and a primary group.
- Users may be added to additional groups (via Add group or Edit group), but the primary group defines the group ownership for all files created by the user (and from which quotas are assigned) under each share.

The NSS has built in support to require hosts to authenticate before the host is able to gain access to the volume. Authentication to a CIFS\SMB Windows share is encrypted. Encryption is done on a volume basis and is not tied to the end station. The NSS supports NTLMv1 authentication, which is an encrypted authentication scheme. When operating within an ADS domain, the Kerberos authentication protocol is used instead of NTLM.

Note

NTLMv2 is more secure encrypted authentication scheme that may be supported in a future NSS release. Note that Vista clients will attempt to use NTLMv2 by default unless explicitly configured otherwise. Vista clients should be configured to use NTLMv1.

Data Integrity and Protection

NSS has some built in capabilities that increase data integrity such as hot swapping, file journaling, hot spares, RAID set failure handling, and Redundant Power Supply Units (RPSU) options. Data protection features include on disk file encryption and volume locking.

RAID Hot Spares

Linksys NSS products support RAID hot spares, which protects data in the event of one or multiple hard drive failures. The hot spare drive (or drives) assigned to mirror data written to the active drives in the NSS system will automatically activate if there is a failure on one or more of the primary drives.

Data Encryption

Linksys NSS supports on-disk data encryption with the 256-bit Advanced Encryption Standard [AES] encryption algorithm. Deploying AES data encryption functionality will allow the business to store traffic on the NSS infrastructure securely without putting sensitive proprietary information at risk in the event that a drive or unit is stolen.

If data encryption is desired, it must be activated during volume creation. It can not be turned on after the volume has been created. A password is used to manage access the data. Passwords must be entered to access an encrypted volume whenever the NSS is started up (after power cycle, shutdown/reboot). The password can be changed at any time.

Warning

Data encryption must be activated during volume creation. Where there is available storage capacity in the array, a volume size may be increased whether encrypted or not. However, it is not possible to reduce the encrypted volume size.

File/Volume Locking

In order to provide an extra layer of security against data theft, encrypted volumes may be administratively locked, which means that the volume is un-mounted from the array and is unusable. Unlocking the volume re-mounts the volume on the array so it can be used.

The password must be entered to unlock an encrypted volume when the NSS is started up following a power interruption, shutdown, reboot, or if the volume was manually locked by the administrator through the NSS configuration interface.

✓	
Recommendation	Because a password is required to decrypt a locked volume, it is highly recommended to maintain a backup of the password to ensure that it is accessible when required. Without the password, there is no way to unlock the volume.

Configurable Network Access Filtering (IP and MAC based)

Access to the NSS can be filtered based on a device's or user's IP or MAC address.

File Transfer Security

The NSS includes an SFTP (Secure File Transfer Protocol) server application that supports Explicit (TLS-based) SFTP as a standards-based method to enable secure transfer of files to and from the NSS over the network.

Anti-Virus

In stand-alone mode, NSS security updates are administered manually like other Linksys Business Series products via signature updates. In the Linksys One mode of operation, the NSS will automatically receive security updates from the Services Router/Service Provider.

Secure Management Protocols

The NSS uses encrypted and secure SNMPv3 for GUI management access for SNMP Gets (though not SNMP Sets). File Transfer access to NSS can be secured by enabling SFTP.

Storage Expansion

The storage solution should offer adequate storage capacity in the near term and suitable expandability into the future. It should also provide the ability to add more capacity without disturbing NAS operations.

Linksys NSS storage expansion options include:

- Adding additional disk drives as individual disks in empty slots
- Adding an additional NAS unit to the network
- Drive set migration (RAID & Volume Encryption/Expansion)
- Network virtualization of volumes between NSS devices

There is no need to configure the additional capacity or to create additional file systems to make the extra capacity available. NSS products can be reconfigured at any time, even hot swapping and resorting hard drives to different storage bays, when a new RAID level or other storage configuration is necessary. RAID sets on one Linksys NSS can migrate to another Linksys NSS device without regard to the order that the hard drive disks are placed in the drive bays.

Warning	Attempting to migrate RAID sets on non-Linksys NSS storage systems can result in RAID set corruption and possibly storage system failure.

Storage Backup

Backup is the activity of copying files or data so that they will be preserved in case of equipment failure or other catastrophe. There are several different storage backup options:

1. Local CIFS backup within the source array (same device) or to a second (or more) LAN attached NSS
2. Remote backup to a remote CIFS server or to a third party storage solution
3. Snapshot, a volume backup with instant access to a previously captured backup

Linksys NSS contains a backup utility that can create full and incremental backups. Directories, files, and folders can be backed up on a configured schedule to other Windows-compatible (CIFS) NAS devices or remote servers. Backups (and restores) are managed by the administrator and are used to archive a specific list of shares for offline or offsite storage. Backup images can be used to recover from a major system failure, such as would be required to restore the shares after repairing a failed disk in a RAID 0 array. Full and incremental backups may be specified, as well as a time interval between scheduled iterations (daily, weekly, monthly). Backups are managed via the 'Backup' utility within the device GUI.

Linksys NSS supports backup for both agent (software)-based and agent-less backup architectures. The NSS does not require the management of agent software. However, a third party agent software product may be used where it supports the ability to use a CIFS or FTP mount point as the backup target. As long as the backup software is not server based, any client based product should work for backups.

Note	In the past, many businesses have used storage applications (e.g. BackupExec, NetBackup) to backup various storage platforms to tape drives. Today, the cost associated with using another NAS as a backup target can be significantly less than the amount of power, floor space and labor required to maintain a tape-based infrastructure.

Local Backup

The local backup options include:

- Local CIFS Backup to another volume/share within the source array on the same device (Figure 15)
- Local CIFS Backup to a second (or more) LAN attached NSS across the LAN (Figure 16)

Using a local source array as backup target can reduce storage costs and recovery time. Linksys NSS can replicate to a duplicate NSS backup target or to any storage platform. It relies on established communication protocols (FTP, CIFS) for backup.

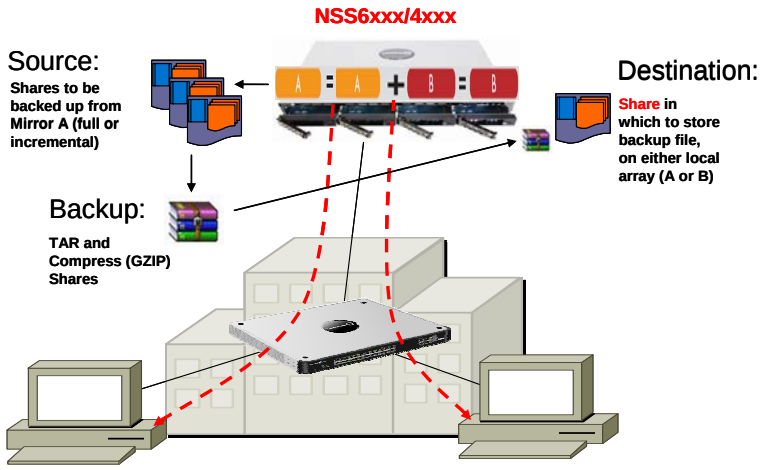

Figure 15: Local CIFS Backup - Same Device

In Figure 15, the administrator uses the 'backup' utility in the NSS GUI menu to select:

- The specific shares for which backup is required
- The frequency of the backup; and
- The target CIFS share on the local system where the backup file is to be written

When the system clock reaches the configured backup time, the system will select those shares, concatenate them into a Tape Archive formatted file and compress that file using GZIP. The compressed file is then written to the target device share.

In Figure 16, the target for the backup is another local NSS device within the CPE infrastructure.

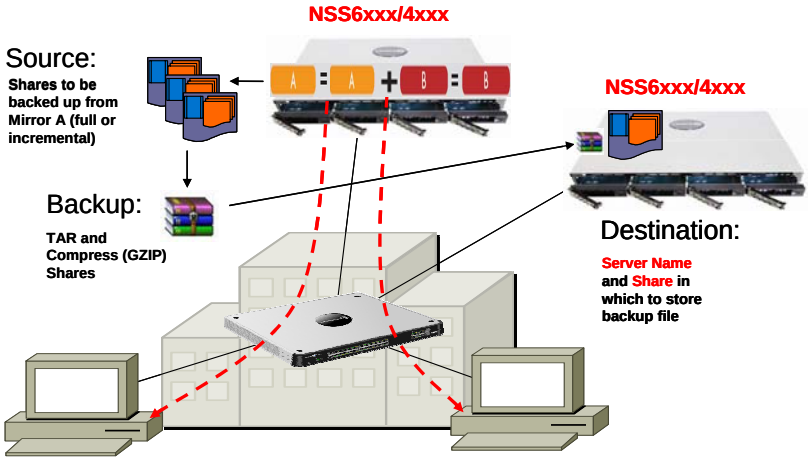

Figure 16: Local CIFS Backup - 2nd (or more) LAN attached NSS

Again in this example, the administrator uses the 'backup' utility in the Device's GUI menu to select the specific shares for which backup is required, the frequency of the backup and the target CIFS share where the backup file is to be written However, this time the target includes a Server name and associated user ID and password. When the system clock reaches the configured backup time, the system will select those shares, concatenate them into a Tape Archive formatted file and compress that file using GZIP. The compressed file is then written to the target device share over the LAN.

Remote Backup

The remote backup options include:

- Remote CIFS Backup to a WAN accessed NSS (Figure 17)
- Remote CIFS Backup to a third party WAN Storage Service via a WAN connection (Figure 18)

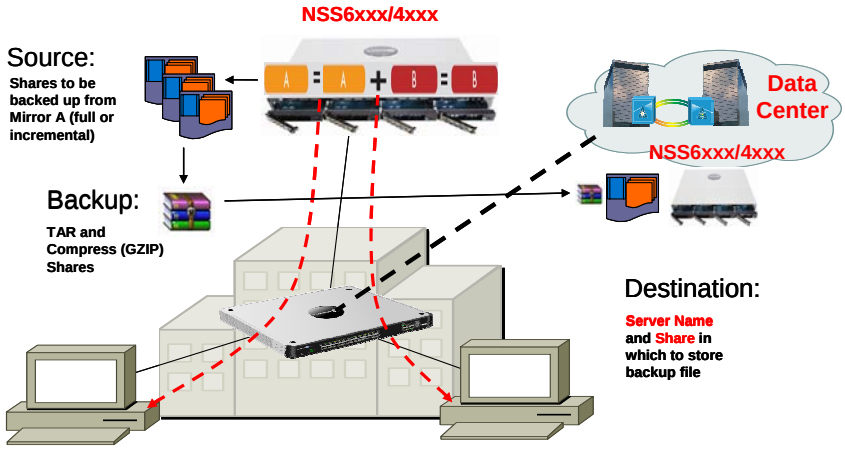

Figure 17: Remote CIFS Backup - WAN accessed NSS

The process for backup to a remote location is fundamentally the same as backup to another NSS device within the CPE infrastructure (illustrated in Figure 16). The target can be any remote storage target such as a NSS device located in a remote data center (e.g. a remote NSS located at the corporate headquarters in a solution for backups of NSS located in satellite offices).

The configuration setup is the same. The administrator uses the 'backup' utility in the source device's GUI menu to select the specific shares for which backup is required, the frequency of the backup and the target CIFS share where the backup file is to be written. Again, the target includes a Server name (and user ID and password). When the system clock reaches the configured backup time, the system will select those shares, concatenate them into a Tape Archive formatted file and compress that file using GZIP. The compressed file is then written to the target device share over the network.

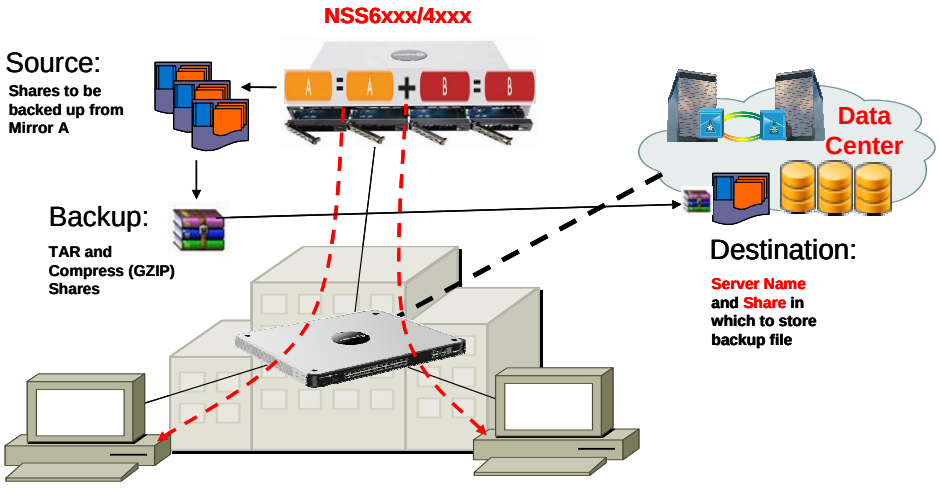

Figure 18: Remote CIFS Backup - WAN Storage Service

Remote CISF backup to a third party WAN storage service is another option that can provide a high value, low cost backup (especially for lots of data). CISF is used for the remote backup. The advantage is that these managed backup services are typically easy and cheap to

to (especially for a lot of data). Backups are regularly sent off-site without user interaction. Data can be encrypted during transmission and storage for more efficient use of bandwidth and storage resources.

CISF allows the user to send files being backed up to a remote designated storage backup site (third party) that is accessed via a WAN connection where that system supports CIFS connections. Most third party backup services provide CISF clients that use efficient backup algorithms.

The required configuration is the same as for a local backup. The administrator uses the 'backup' utility in the source device's GUI menu to select the specific shares for which backup is required, the frequency of the backup and the target CIFS share where the backup file is to be written. The target must still include a Server name (and User ID and Password). When the system clock reaches the configured backup time, the system will select those shares, concatenate them into a Tape Archive formatted file and compress that file using GZIP. The compressed file is then written to the target device share over the network using CIFS.

There are several options to consider with a remote backup:

4. Network bandwidth: The capacity of the WAN link can limit remote backup performance. Depending on the link, an initial full backup can take many days (after that, only changes will be sent), and restoring data can take hours. Typically, bandwidth will be in the 100's of Kilobits/second, versus the LAN-based local CPE copy where the network links are either 100's or 1000's of Megabits/second. Increased bandwidth can be expensive, and for most companies, it's hard to justify making the change for backup alone. But if remote office data is growing fast enough, it's likely that there are other communication problems that would also benefit from a larger link.
5. Backup method: The conventional model is to do daily incremental (changes only) and weekly full backups, which is simple to set up and administer on the Linksys NSS. The drawback to incremental backups is that you risk losing all data created since the last backup, so you should be prepared to perform frequent remote backups. The Linksys NSS' time-organized save sets make it easy to cycle remote backups to off-site storage and bring data back again as needed.

Volume Snapshots

Snapshots are another approach to backing up data. A storage snapshot is a set of reference markers, or pointers, to data stored on a volume. Snapshots streamline access to stored data and can speed up the process of data recovery.

Linksys NSS have a snapshot capability that supports single file restore from an image backup and incremental backups against an image backup (Figure 19). Both features are important.

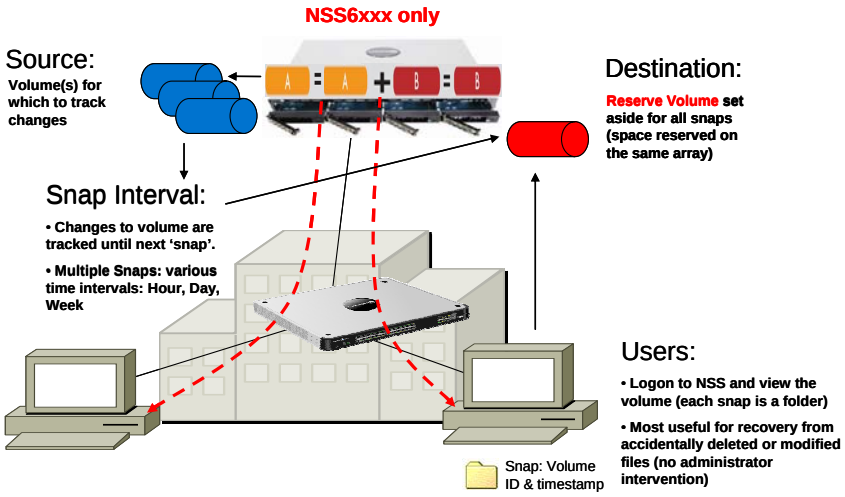

Figure 19: Snapshot

Note

The snapshot feature is only available on the NSS6000 series system.

Snapshots are setup by the administrator, but they are online, i.e. always accessible to users without the need for an administrator to explicitly restore a backup image. They are most useful for recovery from accidental deletion or modification of files.

Operationally, snapshots act like iterative incremental backups of a specified volume. All changes made to the volume that is the target of the snapshot will be stored in a special "snapshot reserve" when the volume is snapped. All subsequent changes are then tracked until the snapshot period expires again and the volume is 'resnapped'. Each time a volume is 'resnapped', the existing snapshot in the reserve is replaced by the current snapshot and the change tracking reference point is reset. It is possible to have multiple snapshots for the same volume with varying time intervals (for example: hourly, daily, weekly snapshots). Each of these snapshots would take up space in the snapshot reserve.

Since snapshots are volume-based, all shares within the selected volume are 'snapped' and stored in the "reserve" volume that is allocated on the array when the snapshot is configured. Administrators need to size the snapshot reserve so that it is large enough to contain all the changes to the volume between resnaps. The more file sharing activity that happens to a given volume and the longer the snapshot interval, the larger the reserve must be. A rule of thumb is 20% of the volume size.

A potential archival strategy utilizing the backup utility in conjunction with snapshots would be to create a full backup of all the shares on a volume and immediately initiate a snapshot schedule to cover the time period until the next scheduled backup. This would establish a baseline reference point for the initial snapshot and allow users to access the snapshot system to recover files without having the administrator restore any backup images.

Because an initial full backup of a system that has a single array capacity of up to 3TB can be a huge amount of data, it may be impractical to attempt a full backup to a remote storage server over a low capacity WAN connection. Therefore, you may want to consider initiating a full backup using a local LAN attached system (either on spare drives within the same system or another NSS system) and then moving those drives to the remote location, re-enabling them in another NSS system and then proceeding with incremental backups. This may be particularly useful for backup of remote office systems to the central office location.

Fortunately, the NSS system has been specifically designed to simplify the process of migrating arrays to a remote NSS device. The basic requirement is to gracefully shutdown the array, remove the disks, move them to the other site, install them in a powered down system and once all the disks are installed, power up the new NSS. The disks can be installed in the new system in any slot or order.

Storage Recovery

In the event of a hard drive disk failure, the Linksys NSS allows users to keep using the remaining disks in the RAID set until the system reaches its pre-configured shutdown period. Network administrators can specify the period of time after failure for access to the system by users so they can schedule failed disk swap-out at an appropriate time.

Data recovery is currently a manual process. In a local backup scenario, backed up data is restored from NSS to NSS as shown in Figure 20:

- Destination NSS: The failed array is repaired, and the volumes and shares are recreated.
- Source NSS: The administrator finds the file on the server name and share in which the backup file was stored
- Administrator: The administrator logs on to the source NSS and mounts the share that contains backup file, then logs on to the destination NSS and mounts the target share for the restore.
- Restore: The file is copied/transfer from the source share to the destination share and the files are extracted (tar.gz).

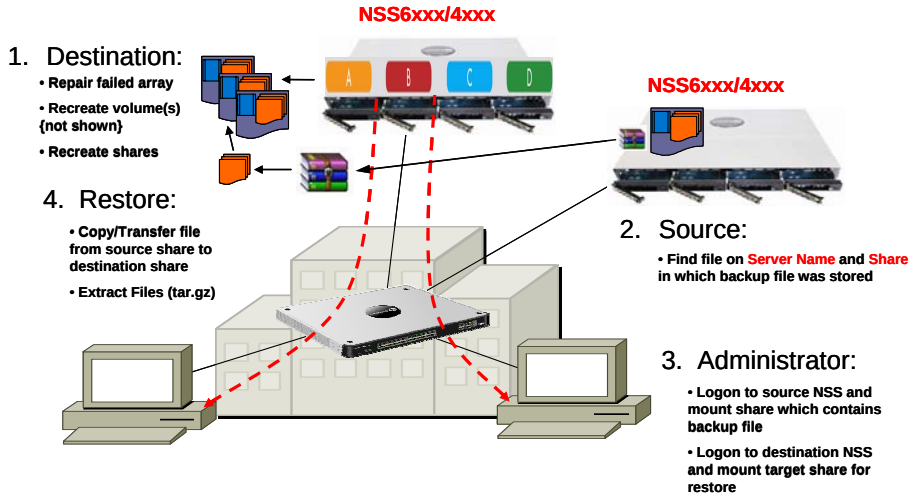

Figure 20: Restore of Backup File

Storage Performance

Availability

The availability options include:

- Hot-swappable NAS chassis: The NSS drive chassis contains a Linux Operating System (OS) that controls the system. Unlike other NAS systems that need to contain operating system software on one or more hard drives, if a drive fails, the NSS system will continue to operate. Network drives can be reconfigured at any time, with the ability to hot swap and re-sort hard drives to different storage bays.

- Hardware based RAID array: Many other SMB and SOHO NAS devices run small processors and software-based RAID. The result is transfer rates that average 10MByte/second, which is quite slow compared to what Linksys NSS systems offer with a hardware based RAID array.
- Hot RAID Spare: A spare hard drive can be designated as a Hot Spare in the event of a disk failure in the RAID set to provide maximum data protection.
- Journaled File System: Linksys NSS products utilize XFS, a journaled file system. A fault-resilient file system provides data integrity because updates to directories and bitmaps are constantly written to a serial log on disk before the original disk log is updated. If the system fails, a full journaling file system restores the data on the disk to its pre-crash configuration. It also recovers unsaved data and stores it in the location where it would have gone if the computer had not crashed.
- Redundant LAN Connections: Dual Gigabit Ethernet (10/100/1000) links facilitate export of virtualized RAID sets and backup operations.
- Staggered Drive Spin-UP: The NSS devices minimize system power supply cost by using a single, sequential hard drive power up or power down in the storage array. Drives are spun up one at a time to minimize spin-up power draw which, in other arrays, can typically be 4 to 5 times the draw on power depending on the number of drives in the array.
- Idle Drive Spin-Down: The NSS devices feature "Idle Drive Spin-Down," which helps to extend the lifespan of the disk drives. This minimizes active drive operation when the NSS device is not being accessed, achieving stated "Mean Time Before Failure."
- SNMP traps (gets only) can be sent to an SNMP-capable network management system. The system also supports remote logging with syslog and system alerts on electrical and mechanical anomalies should they occur (these alerts are visible in the management GUI of the device).
- Optional External Redundant Power Supply and integrated UPS support: RPSU support is available for NSS devices and the NSS can be connected to UPS products.

MTBF

Mean Time Between Failure (MTBF) is a storage performance metric. Linksys NSS devices are designed to increase MTBF with the following capabilities:

- Environmental controls reduce the amount of power consumed (Stagger Drive Spin-UP).
- When drives are not being used, the disks will spin-down to an idle state after some period of time to prevent disk failure (Idle Drive Spin-Down). This increases drive lifespan and saves power. The default spin-down time is set for 8 hours.
- NSS devices are designed to operate with best in class disk drives, which support a business-class requirement for 7x24x365 operation (see Linksys Approved Vendor List for recommended drive manufacturers).

Note

MTBF is not an indicator for how long any particular drive will last and may not necessarily represent storage performance in 'real World' usage. Accordingly, MTBF should not be used as the only metric to assess storage performance. A backup strategy should also be implemented to protect against any drive failure. Note also that use of unsupported drives could result in unpredictable system behavior or data loss.

SMART

SMART (Self-Monitoring, Analysis, and Reporting Technology) captures drive error data to predict failure far enough in advance so you can back up. SMART monitors mechanical failures. There are several SMART parameters where errors are strongly correlated with drive failure including scan errors, reallocation counts, and offline reallocations.

Note

While SMART can warn you about some potential problems, it does not predict the failure of a single drive. Again, a regular backup strategy should be implemented to protect against possible drive failures.

Storage Management

NSS management tools support the NAS hardware deployed across the network infrastructure. NSS devices run their own Linux OS and are managed and configured using integrated software utilities that run with any standard Web browser. This allows storage administrators to easily check NAS status, diagnose issues and make changes to the NAS configuration from any workstation on the LAN.

Unlike pre-configured, third-party OS-based arrays, NSS products can be configured with hard drives in each bay or without any hard drives at all, because the Linux OS and the RAID reside in the chassis of the device. There is no need to install disk utilities and no need for volume management. The entire data store is self-validating. Add a disk to the NSS system and it joins the storage array. No RAID controllers are required – just add the drives.

Note

NSS4000/NSS6000 ship with a drive-less NAS chassis option that does not require complex CD based software installation.

The browser-based configuration GUI simplifies ongoing NAS monitoring and operation, and the system can be remotely managed and monitored via HTTPS. The GUI is fairly simplistic, but still easy to navigate, and it provides access to all configuration options and features inside the NSS. The GUI can be used to identify available storage, handle backup and restore tasks, and handle a variety of other ongoing tasks.

Dual firmware images are supported, simplifying the process for any future upgrades (e.g. upgrade to Linksys One solution).

Hard and soft quotas can be applied to enforce storage limits for users or groups for volumes on drives of the NSS. Soft quotas are a storage watermark that result in warning e-mails to a network administrator and the individual user. Hard quotas are a limit where users will not be allowed to store more data until the administrator increases the quota or some existing files are removed (via archiving or deletion).

Third party generic management tools can be used to provide heterogeneous NSS platform support. When choosing third party management software, it is important to remember that you need software that supports CIFS/FTP for storage backup with NSS. Try to avoid using multiple management tools if possible.

Linksys Differentiation

The Linksys NSS solution comes with many advanced features at relatively low cost including easy software installation and configuration, diskless chassis options with hot-swap SATA drive bays, advanced RAID options, redundant power, dual NICs for redundancy, and easy, fast backup through snapshots. It also includes remote replication to another Linksys NAS, disk encryption and built-in anti-virus scanning (optional). A wide array of RAID types (including RAID 10) are supported along with spanning and JBOD. Client support for Windows, Mac, and Linux is included. Protocol support includes CIFS/SMB, AFP, NFS, HTTP, and FTP.

The key differentiators of the Linksys NSS solution architecture are as follows:

- Highest Feature Set/Lowest Cost Product in its Class: Linksys NSS offers a pre-configured RAID array/NAS solution with a feature set comparable to higher priced solutions. The high end feature set also distinguishes the NSS from entry-level, desktop NAS systems.
- Ease of Use. The Linksys NSS does not require complex CD based software installation. Its browser-based configuration GUI simplifies installation and operation. The browser-based GUI can also be used to see if there are problems, like a drive failure, that you need to fix.
- Data Protection: The diskless chassis based design with encryption enables advanced data protection. Data integrity is assured with features such as XFS journaling file system, hot spare disk capability, and RPSU options for power redundancy. The Linksys NSS solution supports 256-bit AES on-disk encryption of individual volumes, an important data protection feature.
- Resiliency & Flexibility: With Linksys NSS, network drives can be reconfigured at any time, with the ability to hot swap and re-sort hard drives to different storage bays. Expanding storage capacity is as simple as adding more drives or NSS units. NSS also offers migration of RAID sets between systems and secure local and offsite backup options.
- Cost-Effective: Businesses can realize substantial cost savings with a diskless chassis storage architecture when compared with more expensive and inflexible server arrays. The NSS chassis architecture supports options for diskless or populated disk drive bays with Linux OS and RAID residing in the intelligent chassis of the device. Serial ATA (SATA) disk drives provide increased storage efficiency.
- Reduced Total Cost of Ownership: With the Linksys storage solution there is no need to purchase new and pre-configured NAS systems, drives, third-party OS software upgrades, third-party licenses, license renewals, or accessories. Linksys NSS products come pre-integrated with Microsoft Active Directory Integration, hot-swappable drives, hot-spare drives, and much lower power consumption requirements than more expensive, feature-comparable NAS products from other brands. Significant cost savings on energy expenditures can be realized for these always-on devices. The savings deliver a much lower total cost of ownership and quicker return on investment for the budget-conscious business.
- Linksys One Integration/Upgradeability: Linksys NSS devices are Linksys One Ready, so they can be incorporated into a Linksys One network. Each NSS device contains firmware code that enables it to be automatically discovered by a Linksys One Services Router. This further increases the level of investment protection for the business should they later decide to transition to a hosted solution.

- Network Integration: Each Linksys NSS device includes dual Gigabit Ethernet ports with built-in redundancy and advanced LAN functionality. There is support for VLAN mapping and tagging, QoS control and link aggregation.
- Simplified Management: The browser-based configuration GUI simplifies ongoing monitoring and operation.

Conclusion

As the goals of your organization evolve over time, you will need a storage solution that enables your data center to keep pace. A NAS solution should be optimized to scale your services, virtualized infrastructure, and physical infrastructure. This breadth will help ensure that your data center is built on a foundation that will support your needs today and in the future.

The Linksys storage solution described in this white paper will enable you to extend storage networks using a cost-effective Ethernet infrastructure. All the benefits of NAS, including increased storage utilization, local and remote backups, easier addition of incremental storage capacity, management simplification, and reduced overall total cost of ownership (TCO), can be extended to a new range of applications. This flexible storage solution is especially suited for budget-conscious companies that are constantly growing and who would prefer a NAS system that can grow with them.

Note

This paper is one element of the overarching Linksys Connected Office reference architecture so for more information on other subjects Voice deployments, Security, Multi-Site VPNs and many others follow the link to *www.linksys.com*.

Obtaining Technical Assistance

Linksys provides this white paper as a starting point for using Linksys Business Series Products. Linksys partners can obtain online documentation and access to technical support resources on the Linksys Partner Web Site at www.linksys.com, or by opening a case with the Linksys Business Assistance Center (BAC) at: (800) 326-7114.

Appendix A

Table 1 – Pros and Cons of Different RAID Types

RAID Type	Min Disks	Disk Tax	Pros	Cons
RAID 0 - (Striped Set)	2	0%	Ideal For Higher Performance Read or Write. No Disk "Tax". Can Use 100% Of Storage Capacity	No fault tolerance. If one drive fails, the entire array becomes inaccessible.
RAID 1 - (Mirror)	2	50%	100% redundancy data protection. Can survive a single disk failure. Single Disk Performance Read or Write.	High Disk "Tax", 50% of storage capacity is dedicated to protection.
RAID 1 + Spare – (Mirror + Spare)	3	66%	100% redundancy and addition fault-tolerance. Can Survive 2 Disk Failures. Single Disk Performance Read or Write.	Very High Disk "Tax", 66% of total storage capacity is dedicated to protection. The spare disk is not used until a working disk fails.
RAID 5 – (Striped + Parity)	3	25%	Combination of storage capacity and performance, with a high degree (75%) of space usage and some measure of fault-tolerance. Higher read performance than RAID1; similar to RAID 0.	Medium Disk "Tax", 25% of storage capacity is dedicated to protection. Because of the parity that must be calculated, write transactions are somewhat slower than read transactions. It is resource-intensive to rebuild in the event of a disk failure (as compared with RAID 1).
RAID 5 + Spare – (Parity + Spare)	4	50%	Combination of storage capacity and performance, with increased overall system reliability so that when a disk fails within the array, the spare can be used to rebuild the data existing on the failed disk. Sparing helps to minimize the time before a disk rebuild is required, so it minimizes the time that the system is vulnerable to additional drive failure	High Disk "Tax", 50% of storage capacity is dedicated to protection, with a minimum of 4 disks. Because of the parity that must be calculated, write transactions are somewhat slower than read transactions
RAID 10 - (Mirror Then Stripe)	4	50%	Faster Write Performance Than RAID 5 (No Parity Calc). Faster Rebuild Time. This level provides a high degree of redundancy and can be used for latency sensitive applications with high loads due to its faster write speeds than those levels that use parity for calculations. It also increases the overall system reliability so that when a drive within the array fails, the spare can be used to rebuild the data existing on the failed drive.	High Disk "Tax", 50% of storage capacity is dedicated to protection, with a minimum of 4 disks
JBOD – (Linear) - (Just a Bunch of Disks)	n/a	n/a	Disks of varied sizes can form a single logical unit. Unlike RAID 0, if a single drive fails in a JBOD, only the data on the affected drive is lost. In a RAID 0, this usually means the loss of all the data in the array.	There are no performance benefits and there is no data protection.

LINKSYS®
A Division of Cisco Systems, Inc.

Corporate Headquarters
Linksys, a Division of Cisco
121 Theory
Irvine, CA 92617-3045
USA
http://www.linksys.com
Tel: (800) 546-5797
Fax: (949) 823-3007

European Headquarters
Cisco Systems Europe
11 Rue Camille Desmoulins
92782 Issy-Les-Moulineaux
Cedex 9
France
www-europe.cisco.com
Tel: 33 1 58 04 60 00
Fax: 33 1 58 04 61 00

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-7660
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems Australia, Pty., Ltd
Level 9, 80 Pacific Highway
P.O. Box 469
North Sydney
NSW 2060 Australia
www.cisco.com
Tel: +61 2 8448 7100
Fax: +61 2 9957 4350

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on the

Cisco-Linksys Web site at www.linksys.com.

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China • Colombia • Costa Rica • Croatia • Czech Republic Denmark • Dubai, UAE Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia • Ireland • Israel • Italy • Japan • Korea • Luxembourg • Malaysia • Mexico The Netherlands • New Zealand • Norway • Peru • Philippines • Poland • Portugal • Puerto Rico • Romania • Russia • Saudi Arabia • Singapore • Slovakia • Slovenia South Africa • Spain • Sweden • Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe