NETWORK SECURITY

DISASTER AND RECOVERY

NOTES

INTRODUCTION

Online connectivity during normal day-to-day life is important. We do ordinary tasks such as checking emails, checking the weather and traffic, and using social media to see what friends and family are doing. Additionally, we also use internet connectivity check more sensitive information such as our bank accounts, pay bills online, and transfer money.

NETWORK DISASTER

- Network disaster is a disaster in which the day to day access to the network device and data is disrupted.
- *It also damages the network components such as:*
  - ✓ Data devices
  - ✓ Media
  - ✓ Software
  - ✓ Hardware

- **REASON OF NETWORK DISASTER**
  - ✓ Cabling
  - ✓ Topology failure

CABLING:

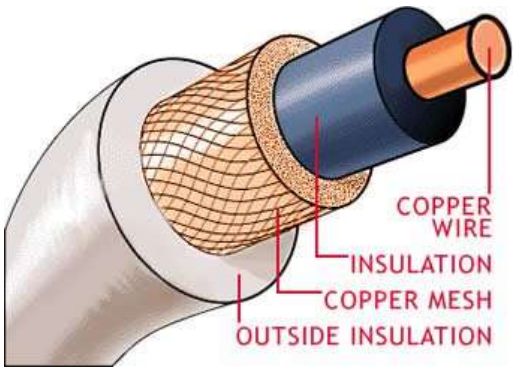
- Cabling is the medium through which information usually moves from one network device to another.
- There are several types of cable which are commonly used with LANs.
- In some cases, a network will utilize only one type of cable, other networks will use a variety of cable types.
- The type of cable chosen for a network is related to the network's topology, protocol, and size.

COAXIAL CABLE:

- Sometimes known as coax cable, is an electrical cable which transmits radio frequency (RF) signals from one point to another.

Working

- Coaxial cable works by carrying data in the centre conductor, while the surrounding layers of shielding stop any signal loss (also called attenuation loss) and help reduce EMI.



- The first layer, called the dielectric, provides distance between the core conductor and the outer layers, as well as some insulation.
- The next layers, collectively referred to as the shield, keep electrical impulses and radio transmissions out.

Advantages of coaxial cable

- ✓ Inexpensive
- ✓ Easy to wire and install
- ✓ Easy to expand
- ✓ Good resistance to EMI
- ✓ Up to 10Mbps capacity
- ✓ Durable

Disadvantages of coaxial cable

- ✓ The main disadvantage of using coaxial cable is that single cable failure can take down an entire network.

TWISTED-PAIR CABLE:

- A **twisted-pair cable** is a cable made by intertwining two separate insulated wires.

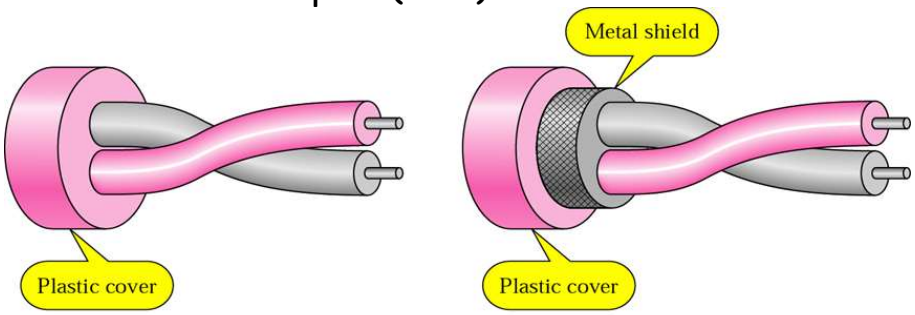
The illustration gives an example of how the inside of these looks.

- Twisted pair cable is a type of wire in which the two conductors of a single circuit are twisted together for the purpose of cancelling out the **electromagnetic interference** from the external sources.

Types of twisted pair cables

The two commonly used types of twisted pair cables are as follows:

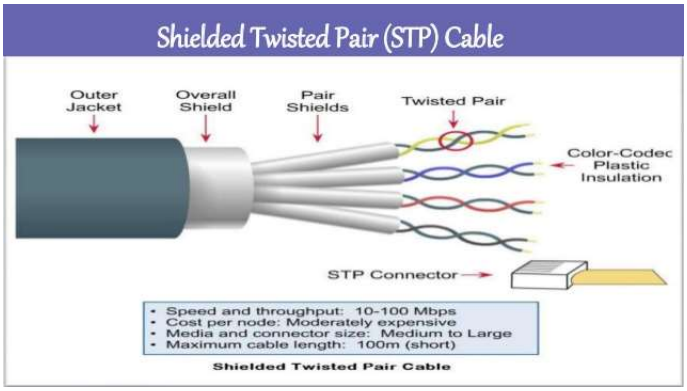
- ✓ Unshielded twisted pair (UTP)
- ✓ Shielded twisted pair (STP)



a. UTP b. STP

STP

- cable has a metal foil or braided mesh covering that mainly encases each pair of insulated conductors.
- Although metal casing improves the quality of the cable by preventing the penetration of noise or the crosstalk , it is bulkier and more expensive.



- This is known as the metal shield which is normally connected to ground so as to reduce the interference of the noise.
- But this makes the cable bulky and expensive. So practically UTP is more used than STP.

Advantages of Shielded Twisted Pair Cable

- Easy to install
- Performance is adequate

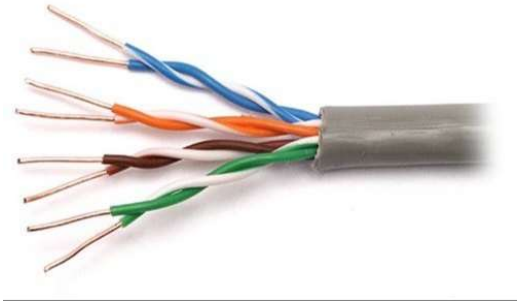
- Can be used for Analog or Digital transmission
- Increases the signalling rate
- Higher capacity than unshielded twisted pair
- Eliminates crosstalk

Disadvantages of Shielded Twisted Pair Cable

- Difficult to manufacture
- Heavy

UTP

- A twisted pair consists of two insulated conductor twisted together in the shape of a spiral as shown in figure .
- The **unshielded twisted pair** cables are generally very cheap and easy to install.
- But they are badly affected by the electromagnetic noise interference.
- In a balanced pair operation the two wires carry equal and opposite signals and the destination detects the differences between the two .
- Number of twists per unit length will then determine the quality of cable. More twists thus means better quality.



Advantages of Unshielded Twisted Pair Cable

- ✓ Installation is easy
- ✓ Flexible
- ✓ Cheap
- ✓ It has high speed capacity,
- ✓ 100 meter limit
- ✓ Higher grades of UTP are used in LAN technologies like Ethernet.

Disadvantages of Unshielded Twisted Pair Cable

- ✓ Bandwidth is low when compared with Coaxial Cable

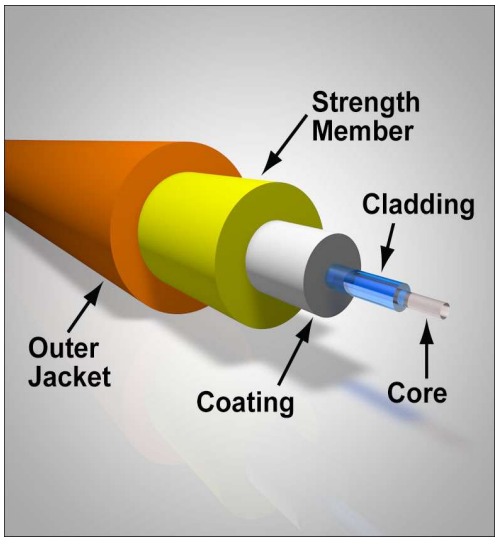
- ✓ Provides less protection from interference.

OPTICAL FIBER:

- An **optical fiber** is a thin fiber of glass or plastic that can carry light from one end to the other.
- The study of optical fibers is called **fiber optics**
- Optical fibers are mainly used in telecommunications, but they are also used for lighting, sensors, toys, and special cameras for seeing inside small spaces.
- They are sometimes used in medicine to see inside people

Working

- An optical fiber is a long, thin strand of clear material.
- Its shape is usually similar to a cylinder.
- In the center, it has a *core*. Around the core is a layer called the *cladding*.
- The core and cladding are made of different kinds of glass or plastic, so that light travels slower in the core than it does in the cladding.
- If the light in the core hits the edge of the cladding at a shallow angle, it bounces off. Light can travel inside the core and bounce off of the cladding.



- No light escapes until it comes to the end of the fiber, unless the fiber is bent sharply or stretched.

If the cladding of the fiber is scratched, it may break. A plastic coating called the buffer covers the cladding to protect it. Often, the buffered fiber is put inside an even tougher layer, called the jacket. This makes it easy to use the fiber without breaking it.

TOPOLOGY

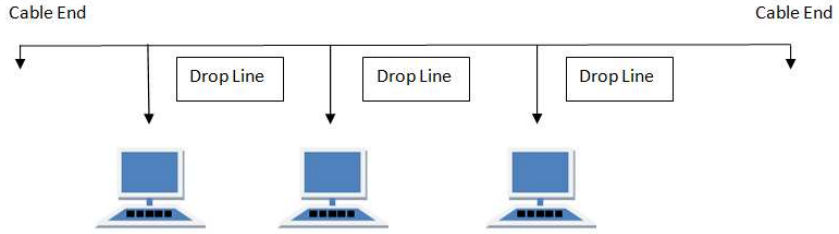
Network Topology is the schematic description of a network arrangement, connecting various nodes(sender and receiver) through lines of connection.

Types of topologies

- ## *LAN TOPOLIGIES*

  - **BUS Topology**

    Bus topology is a network type in which every computer and network device is connected to single cable. When it has exactly two endpoints, then it is called **Linear Bus topology**.



Features of Bus Topology

1. It transmits data only in one direction.
2. Every device is connected to a single cable

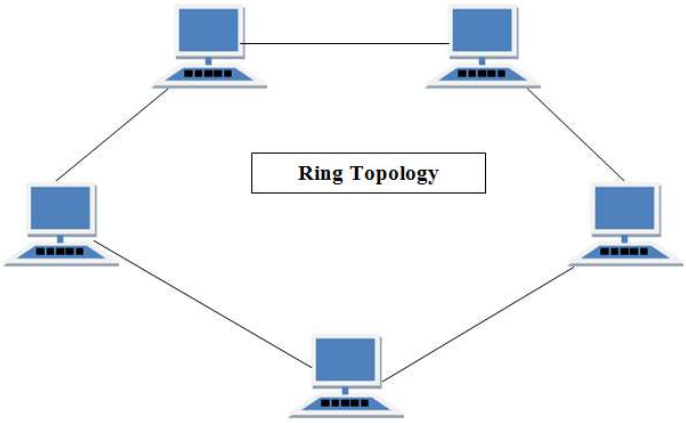
Advantages of Bus Topology

1. It is cost effective.
2. Cable required is least compared to other network topology.
3. Used in small networks.
4. It is easy to understand.
5. Easy to expand joining two cables together.

Disadvantages of Bus Topology

1. Cables fails then whole network fails.
2. If network traffic is heavy or nodes are more the performance of the network decreases.
3. Cable has a limited length.
4. It is slower than the ring topology.

- **RING Topology**



It is called ring topology because it forms a ring as each computer is connected to another computer, with the last one connected to the first. Exactly two neighbours for each device.

Features of Ring Topology

1. A number of repeaters are used for Ring topology with large number of nodes, because if someone wants to send some data to the last node in the ring topology with 100 nodes, then the data will have to pass through 99 nodes to reach the 100th node. Hence to prevent data loss repeaters are used in the network.
2. The transmission is unidirectional, but it can be made bidirectional by having 2 connections between each Network Node, it is called **Dual Ring Topology**.
3. In Dual Ring Topology, two ring networks are formed, and data flow is in opposite direction in them. Also, if one ring fails, the second ring can act as a backup, to keep the network up.
4. Data is transferred in a sequential manner that is bit by bit. Data transmitted, has to pass through each node of the network, till the destination node.

Advantages of Ring Topology

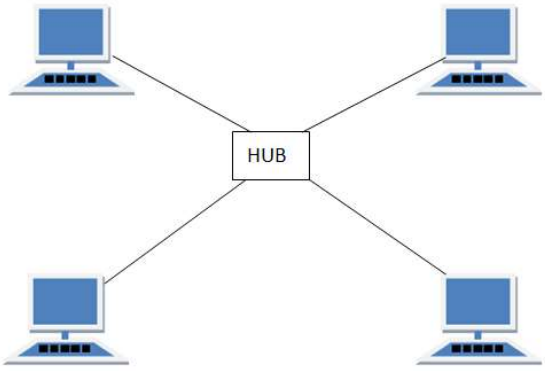
1. Transmitting network is not affected by high traffic or by adding more nodes, as only the nodes having tokens can transmit data.
2. Cheap to install and expand

Disadvantages of Ring Topology

1. Troubleshooting is difficult in ring topology.
2. Adding or deleting the computers disturbs the network activity.
3. Failure of one computer disturbs the whole network.

○ STAR Topology

In this type of topology all the computers are connected to a single hub through a cable. This hub is the central node and all others nodes are connected to the central node.



Features of Star Topology

1. Every node has its own dedicated connection to the hub.
2. Hub acts as a repeater for data flow.
3. Can be used with twisted pair, Optical Fibre or coaxial cable.

Advantages of Star Topology

1. Fast performance with few nodes and low network traffic.
2. Hub can be upgraded easily.
3. Easy to troubleshoot.
4. Easy to setup and modify.
5. Only that node is affected which has failed, rest of the nodes can work smoothly.

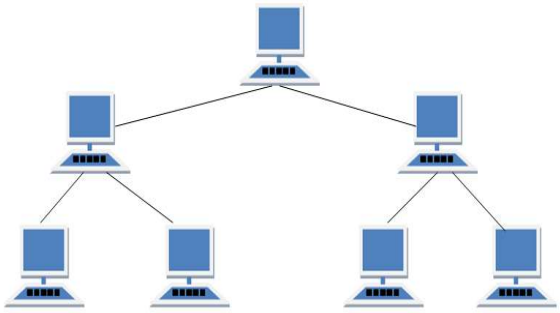
Disadvantages of Star Topology

1. Cost of installation is high.
2. Expensive to use.
3. If the hub fails then the whole network is stopped because all the nodes depend on the hub.

4. Performance is based on the hub that is it depends on its capacity

○ TREE Topology

It has a root node and all other nodes are connected to it forming a hierarchy. It is also called hierarchical topology. It should at least have three levels to the hierarchy.



Features of Tree Topology

1. Ideal if workstations are located in groups.
2. Used in Wide Area Network.

Advantages of Tree Topology

1. Extension of bus and star topologies.
2. Expansion of nodes is possible and easy.
3. Easily managed and maintained.
4. Error detection is easily done.

Disadvantages of Tree Topology

1. Heavily cabled.
2. Costly.
3. If more nodes are added maintenance is difficult.
4. Central hub fails, network fails.

➢ WAN TOPOLOGIES:

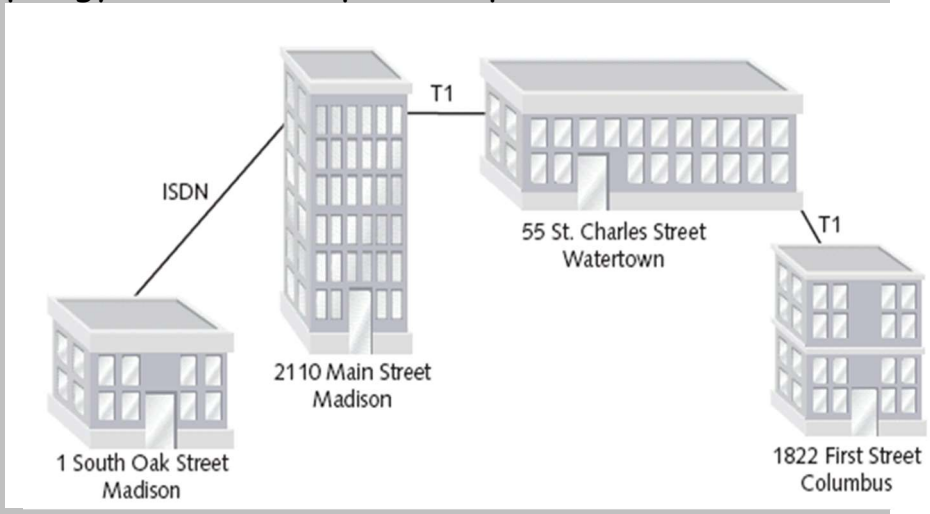
WAN topologies use both LAN add enterprise-wide topologies as building blocks, but add more complexity because of the distance they must cover,

the larger number of users they serve, and the heavy traffic they often handle.

- **Peer-to-Peer**

A WAN with single interconnection points for each location is arranged in a peer-to-peer topology.

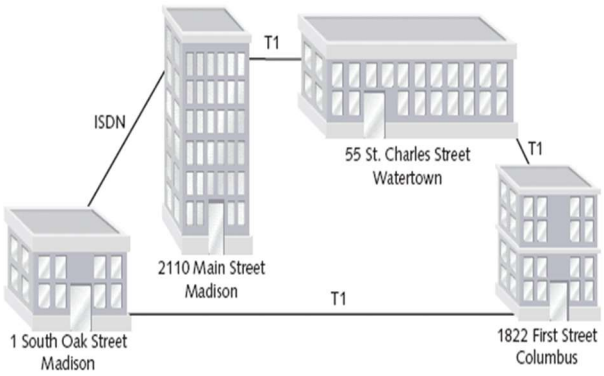
A WAN peer-to-peer topology is similar to peer-to-peer communications on a LAN in that each site depends on every other site in the network to transmit and receive its traffic.



However, the peer-to-peer LANs use computers with shared access to one cable, whereas the WAN peer-to-peer topology uses different locations, each one connected to another one through dedicated circuits.

- **RING**

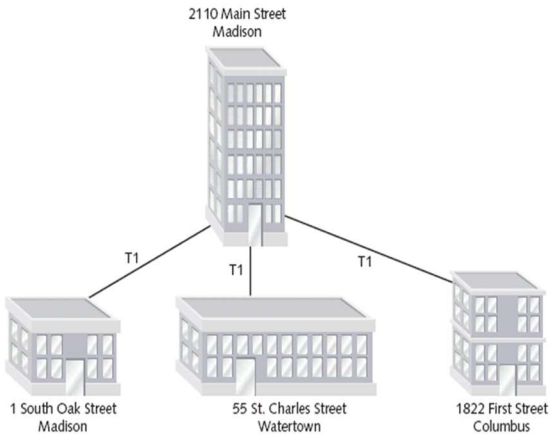
- ✓ In a ring WAN topology, each site is connected to two other sites so that the entire WAN forms a ring pattern.
- ✓ This architecture is similar to the ring LAN topology, except that a ring WAN topology connects locations rather than local nodes.



- ✓ The advantages of a ring WAN over a peer-to-peer WAN are twofold: a single cable problem will not affect the entire network, and routers at any site can redirect data to another route if one route becomes too busy.

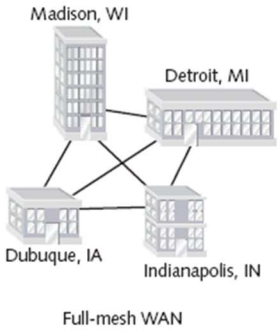
- **STAR**

- ✓ The star WAN topology mimics the arrangement of a star LAN.
- ✓ A single site acts as the central connection point for several other points.
- ✓ This arrangement provides separate routes for data between any two sites.
- ✓ As a result, star WANs are more reliable than the peer-to-peer or ring WANs.

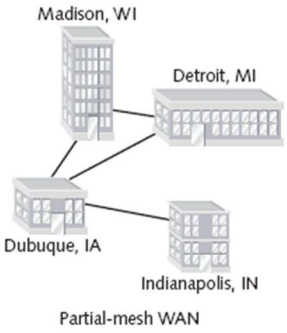


Mesh

- ✓ Like an enterprise-wide mesh, a mesh WAN topology incorporates many directly interconnected nodes--in this case, geographical locations.
- ✓ Because every site is interconnected, data can travel directly from its origin to its destination.
- ✓ If one connection suffers a problem, routers can redirect data easily and quickly.



Full-mesh WAN



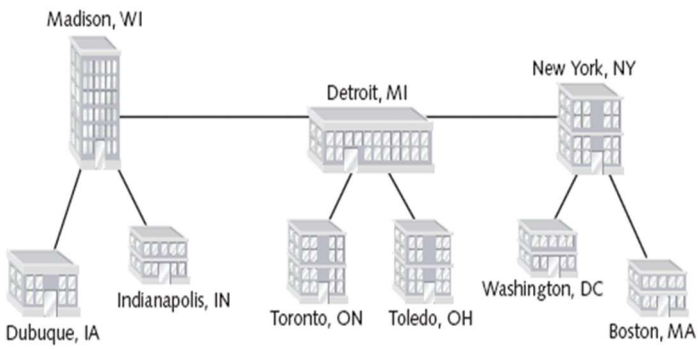
Partial-mesh WAN

- ✓ Mesh WANs are the most fault-tolerant type of WAN configuration because they provide multiple routes for data to follow between any two points.

One drawback to a mesh WAN is the cost.

TIERED

- ✓ Tiered WAN topologies are similar to the hierarchical hybrid topologies used with LANs.
- ✓ In a tiered WAN topology, WAN sites connected in a star or ring formations are



interconnected at different levels, with the interconnection points being organized into layers.

- ✓ Indeed, flexibility makes the tiered approach quite practical.
- ✓ A network architect can determine the best placement of top-level routers based on traffic patterns or critical data paths.
- ✓ In addition, tiered systems allow for easy expansion and inclusion of redundant links to support growth.

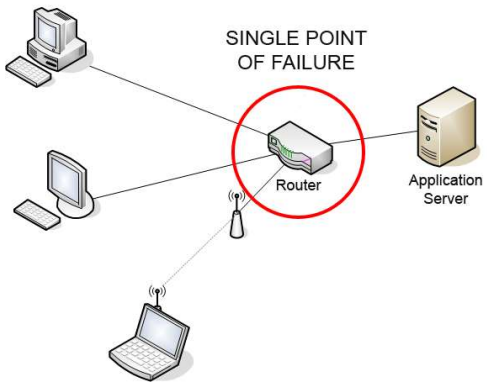
SINGLE POINT OF FAILURE

A **single point of failure**, also known as **SPOF**, is any component of a system that causes the whole system to stop working if it fails. When designing reliable systems, SPOFs can be avoided by implementing redundant components and replicating critical parts of the system.

working

Let's say there's only one server set up to run a particular application. If that server fails, users are unable to access the application.

This single point (the server) has brought access to the application to a halt. People can't work without access to the network.



"a single point of failure can compromise the availability of workloads — or the entire data center — depending on the location and interdependencies involved in the failure." Productivity suffers when systems with SPOFs go down. Security is compromised.

SAVE CONFIGURATION FILE:

If you make a new configuration file or change a current configuration file and want your changes to take effect on the Firebox, you must save the configuration file directly to the Firebox.

You can also save the current configuration file to any local drive or any network drive to which your management computer can connect.

If you plan to make one or more major changes to your configuration file, we recommend that you save a copy of the old configuration file first.

If you have problems with your new configuration, you can restore the old version.

- **Save a Configuration File Directly to the Device**

  You can use Policy Manager to save your configuration file directly to the Firebox.

  a. Select **File > Save > To Firebox**.
     The Save to Firebox dialog box appears.
  b. In the **IP Address or Name** text box, type or select an IP address or name. If you use a name, the name must resolve through DNS. When you type an IP address, type all the numbers and the periods. Do not use the TAB or arrow keys.
  c. In the **Administrator User Name** and **Administrator Passphrase** text boxes, type the credentials for a Device Administrator (read-write) user account.
  d. From the **Authentication Server** drop-down list, select the correct authentication server for the user account you specified.
  e. If you use an Active Directory server for authentication, in the **Domain** text box, type the domain name of your Active Directory server.
  f. Click **OK**.

❖ Save a Configuration File to a Local or Network Drive

You can use Policy Manager to save your configuration file to a local or network drive.

1. Select **File > Save > As File**.
   You can also use CTRL-S. A standard Windows save file dialog box appears.

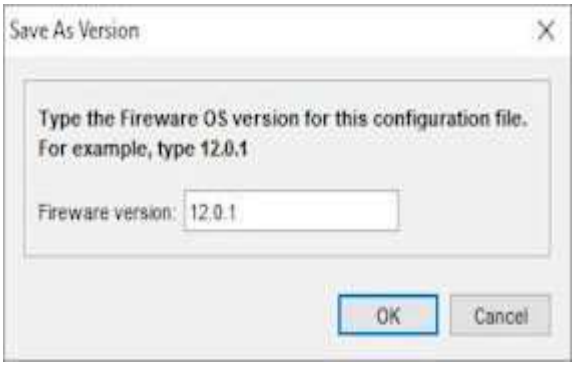
2. Type the name of the file.

   The default location is the `My Documents\My WatchGuard\configs` directory. You can also save the file in any folder you can connect to from the management computer. For better security, we recommend that you save the files in a safe folder that no other users can get access to.

3. Click **Save**.
   The configuration file is saved to the directory you specify.

❖ Save a Configuration File for a Specific Fireware Version

You can use Policy Manager to save a configuration file for a specific Fireware version. This is useful when you want to create a configuration file for Rapid Deploy or save a configuration file for a Firebox with a different version of Fireware.



To save the configuration file for a specific Fireware version:

1. Select **File > Save > As Version**.
   The Save As Version dialog box appears.

2. Type the Fireware OS version for the configuration file.
   The version you specify must be in the range of versions in the configured OS Compatibility settings.
   For information about compatibility settings, see Configure Fireware OS Compatibility.

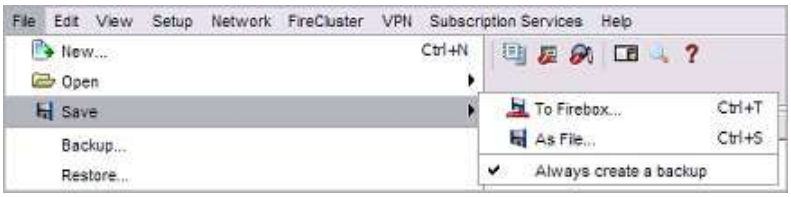
3. Click **OK**.
   If any feature in the configuration is not compatible with the version you specify, an error message appears with information about what you must change before you can save the configuration as the specified version.

❖ Automatically Create Configuration File Backups

Each time you save configuration changes to a local file, the file replaces the previous copy of the file. You can configure Policy Manager to automatically save a backup copy of the configuration file each time you save changes to a file. The backup copy includes a timestamp in the file name. This makes it easier for you to keep a record of the configuration changes made over time. This backup option is not enabled by default.

To enable the automatic creation of backup configuration files:

1. Select **File > Save**.



2. Select **Always create a backup**.
   Adjacent to Always create a backup, a check mark appears.

3. To verify the feature is enabled, select **File > Save**.

4. Make sure a check mark appears adjacent to the **Always create a backup** menu item.
   A check mark appears only when the option is enabled.

After you enable the backup option, each time you save the configuration to a file, Policy Manager saves a second copy of the configuration file in the same location, with the date and timestamp added to the file name. The backup file name includes the original file name, plus the date (year-month-day) and the time (hour-minute-second).

UPS

- ✓ An **uninterruptible power supply** or **uninterruptible power source** (**UPS**) is an electrical apparatus that provides emergency power to a load when the input power source or mains power fails.
- ✓ A UPS differs from an auxiliary or emergency power system or standby generator in that it will provide near-instantaneous protection from input power interruptions, by supplying energy stored in batteries, supercapacitors, or flywheels.
- ✓ The on-battery run-time of most uninterruptible power sources is relatively short (only a few minutes) but sufficient to start a standby power source or properly shut down the protected equipment. It is a type of continual power system.
- ✓ A UPS is typically used to protect hardware such as computers, data centers, telecommunication equipment or other electrical equipment where an unexpected power disruption could cause injuries, fatalities, serious business disruption or data loss.

RAID

- ✓ **RAID** (**Redundant Array of Inexpensive Disks** or Drives, or **Redundant Array of Independent Disks**) is a data storage virtualization technology that combines multiple physical disk drive components into one or more logical units for the purposes of data redundancy, performance improvement, or both.
- ✓ This was in contrast to the previous concept of highly reliable mainframe disk drives referred to as "single large expensive disk" (SLED).
- ✓ Data is distributed across the drives in one of several ways, referred to as RAID levels, depending on the required level of redundancy and performance. The different schemes, or data distribution layouts, are named by the word "RAID" followed by a number, for example RAID 0 or RAID 1. Each scheme, or RAID level, provides a different balance among the key goals: reliability, availability, performance, and capacity.

- ✓ RAID levels greater than RAID 0 provide protection against unrecoverable sector read errors, as well as against failures of whole physical drives.

LEVELS:

RAID 0

- ✓ RAID 0 consists of striping, but no mirroring or parity. Compared to a spanned volume, the capacity of a RAID 0 volume is the same; it is the sum of the capacities of the disks in the set. But because striping distributes the contents of each file among all disks in the set, the failure of any disk causes all files, the entire RAID 0 volume, to be lost.

- ✓ A broken spanned volume at least preserves the files on the unfailing disks.

- ✓ The benefit of RAID 0 is that the throughput of read and write operations to any file is multiplied by the number of disks because, unlike spanned volumes, reads and writes are done concurrently, and the cost is complete vulnerability to drive failures.
- ✓ Indeed, the average failure rate is worse than that of an equivalent single non-RAID drive.

RAID 1

- ✓ RAID 1 consists of data mirroring, without parity or striping.

- ✓ Data is written identically to two drives, thereby producing a "mirrored set" of drives. Thus, any read request can be serviced by any drive in the set.

- ✓ If a request is broadcast to every drive in the set, it can be serviced by the drive that accesses the data first (depending on its seek time and rotational latency), improving performance. Sustained read throughput, if the controller or software is optimized for it, approaches the sum of throughputs of every drive in the set, just as for RAID 0.

- ✓ Actual read throughput of most RAID 1 implementations is slower than the fastest drive. Write throughput is always slower because every drive must be updated, and the slowest drive limits the write performance. The array continues to operate as long as at least one drive is functioning.[12]

RAID 2

- ✓ RAID 2 consists of bit-level striping with dedicated Hamming-code parity.

- ✓ All disk spindle rotation is synchronized and data is striped such that each sequential bit is on a different drive. Hamming-code parity is calculated across corresponding bits and stored on at least one parity drive.

- ✓ This level is of historical significance only; although it was used on some early machines (for example, the Thinking Machines CM-2), as of 2014 it is not used by any commercially available system.

RAID 3

- ✓ RAID 3 consists of byte-level striping with dedicated parity.

- ✓ All disk spindle rotation is synchronized and data is striped such that each sequential byte is on a different drive.

- ✓ Parity is calculated across corresponding bytes and stored on a dedicated parity drive. Although implementations exist, RAID 3 is not commonly used in practice.

RAID 4

- ✓ RAID 4 consists of block-level striping with dedicated parity.

- ✓ This level was previously used by NetApp, but has now been largely replaced by a proprietary implementation of RAID 4 with two parity disks, called RAID-DP.

- ✓ The main advantage of RAID 4 over RAID 2 and 3 is I/O parallelism: in RAID 2 and 3, a single read I/O operation requires

reading the whole group of data drives, while in RAID 4 one I/O read operation does not have to spread across all data drives.

- ✓ As a result, more I/O operations can be executed in parallel, improving the performance of small transfers.[3]

RAID 5

- ✓ RAID 5 consists of block-level striping with distributed parity.
- ✓ Unlike RAID 4, parity information is distributed among the drives, requiring all drives but one to be present to operate.
- ✓ Upon failure of a single drive, subsequent reads can be calculated from the distributed parity such that no data is lost. RAID 5 requires at least three disks.
- ✓ Like all single-parity concepts, large RAID 5 implementations are susceptible to system failures because of trends regarding array rebuild time and the chance of drive failure during rebuild (see "Increasing rebuild time and failure probability" section, below).
- ✓ Rebuilding an array requires reading all data from all disks, opening a chance for a second drive failure and the loss of the entire array.

RAID 6

- ✓ RAID 6 consists of block-level striping with double distributed parity.
- ✓ Double parity provides fault tolerance up to two failed drives. This makes larger RAID groups more practical, especially for high-availability systems, as large-capacity drives take longer to restore. RAID 6 requires a minimum of four disks.
- ✓ As with RAID 5, a single drive failure results in reduced performance of the entire array until the failed drive has been replaced. With a RAID 6 array, using drives from multiple sources and manufacturers, it is possible to mitigate most of the problems associated with RAID 5.

- ✓ The larger the drive capacities and the larger the array size, the more important it becomes to choose RAID 6 instead of RAID 5.[24] RAID 10 also minimizes these problems.

CLUSTERING

Clustering is the task of dividing the population or data points into a number of groups such that data points in the same groups are more similar to other data points in the same group and dissimilar to the data points in other groups. It is basically a collection of objects on the basis of similarity and dissimilarity between them.

Let's understand this with an example. Suppose, you are the head of a rental store and wish to understand preferences of your costumers to scale up your business. Is it possible for you to look at details of each costumer and devise a unique business strategy for each one of them? Definitely not. But, what you can do is to cluster all of your costumers into say 10 groups based on their purchasing habits and use a separate strategy for costumers in each of these 10 groups. And this is what we call clustering.

BACKUP

A **backup** is a copy of important data that is stored on an alternative location, so it can be recovered if deleted or it becomes corrupted. Depending on how often the data changes, how valuable it is, and how long it takes to back up determines how often to backup.
Today, there are several ways to back up your information and mediums to keep your data. For example, CD-R, DVD-R, USB thumb drives, external drives, and in the cloud are some of the most popular places to backup your data.

Why should I back up data?

A computer could stop working at any time, and data on a hard drive could become corrupted or lost if the

hard drive fails. When hardware or the computer stops working, data on the computer could be lost. Any important files should be backed up to prevent loss of data and ensure you can recover those files if needed.

Types of backup

Local Backup

Local backups are any kind of backup where the storage medium is kept close at hand or in the same building as the source. It could be a backup done on a second internal hard drive, an attached external hard drive, CD/ DVD –ROM or Network Attached Storage (NAS). Local backups protect digital content from hard drive failures and virus attacks. They also provide protection from accidental mistakes or deletes. Since the backups are always close at hand they are fast and convenient to restore.

Offsite Backup

When the backup storage media is kept at a different geographic location from the source, this is known as an offsite backup. The backup may be done locally at first but once the storage medium is brought to another location, it becomes an offsite backup. Examples of offsite backup include taking the backup media or hard drive home, to another office building or to a bank safe deposit box.

Beside the same protection offered by local backups, offsite backups provide additional protection from theft, fire, floods and other natural disasters. Putting the backup media in the next room as the source would not be considered an offsite backup as the backup does not offer protection from theft, fire, floods and other natural disasters.

Online Backup

These are backups that are ongoing or done continuously or frequently to a storage medium that is always connected to the source being backed up. Typically the storage medium is located offsite and connected to the backup source by a network or Internet connection. It does not involve human intervention to plug in drives and storage media for backups to run. Many commercial data centres now offer this as a subscription service to

consumers. The storage data centres are located away from the source being backed up and the data is sent from the source to the storage data centre securely over the Internet.

Remote Backup

Remote backups are a form of offsite backup with a difference being that you can access, restore or administer the backups while located at your source location or other location. You do not need to be physically present at the backup storage facility to access the backups. For example, putting your backup hard drive at your bank safe deposit box would not be considered a remote backup. You cannot administer it without making a trip to the bank. Online backups are usually considered remote backups as well.

Cloud Backup

This term is often used interchangeably with Online Backup and Remote Backup. It is where data is backed up to a service or storage facility connected over the Internet. With the proper login credentials, that backup can then be accessed or restored from any other computer with Internet Access.

RECOVERY

Recovery of lost data can be performed on the verity of storage media's including a hard disk drive, solid state drive, USB, laptop or desktop internal hard drive, Flash drive, Memory or SD cards, etc. Different storage devices have one thing in common; they carries set of electronic equipment which may abruptly fail, become damaged or simply stops working and all the stored data may be compromised. Data recovery will look for the desired files around the storage area of aforementioned storage devices and recover them successfully even if the drive stops working or cannot be normally accessed.

Data recovery process

- Evaluate
- Estimate
- Mirror
- Repair
- Recover
- Analyse
- Return