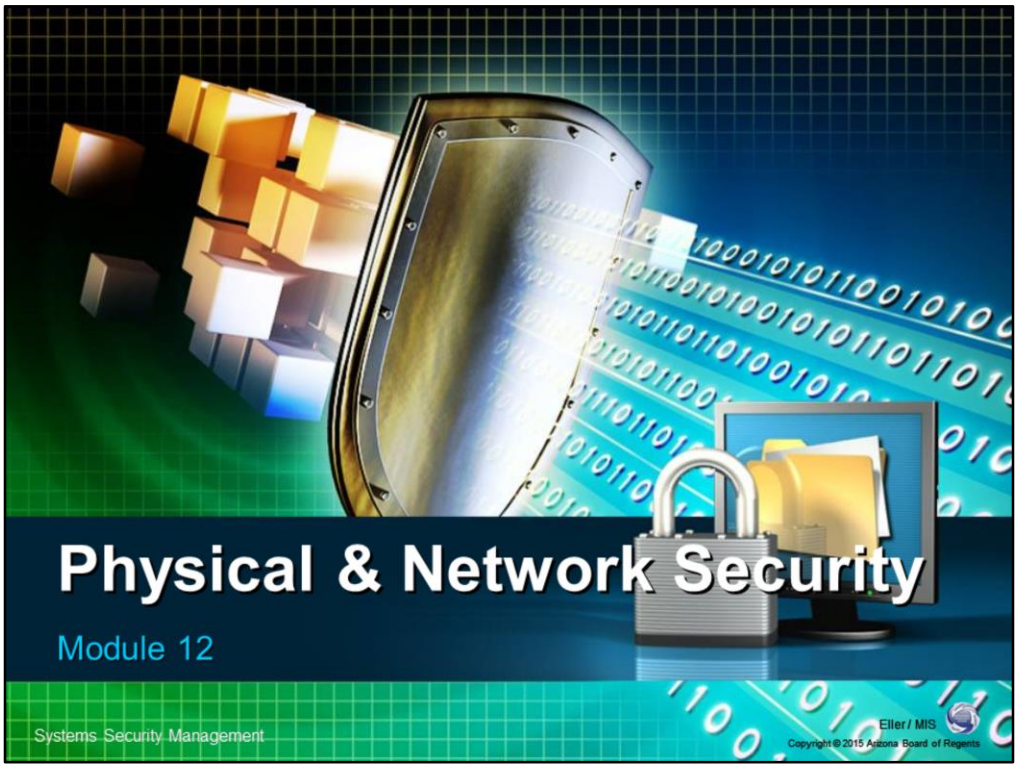
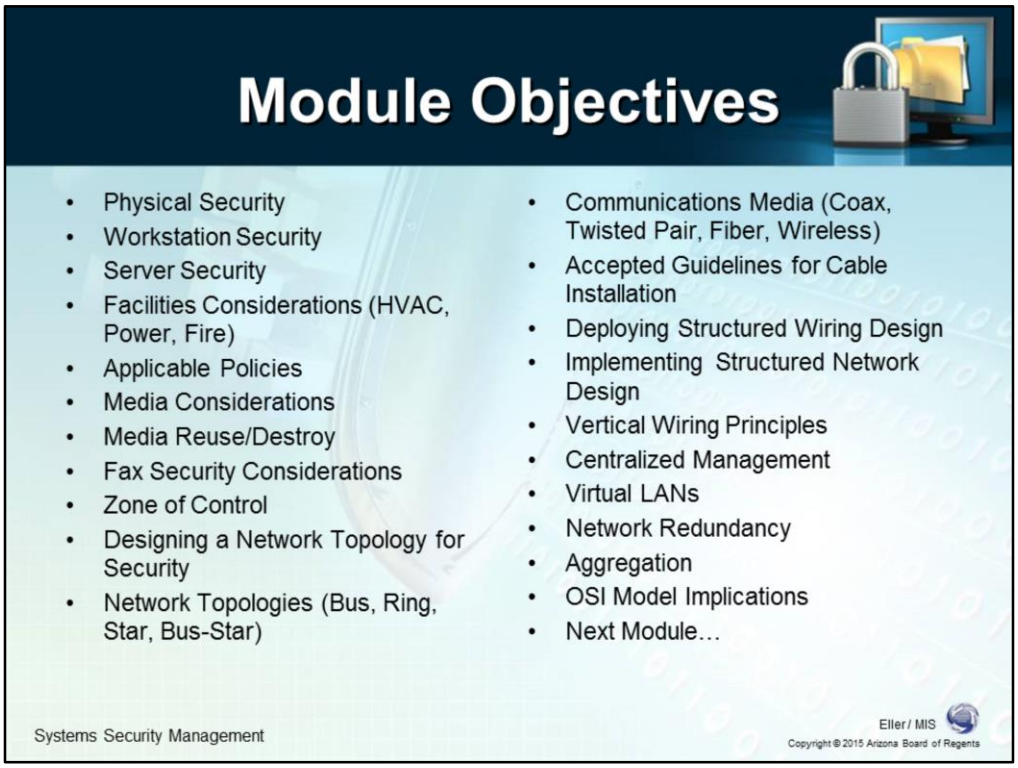
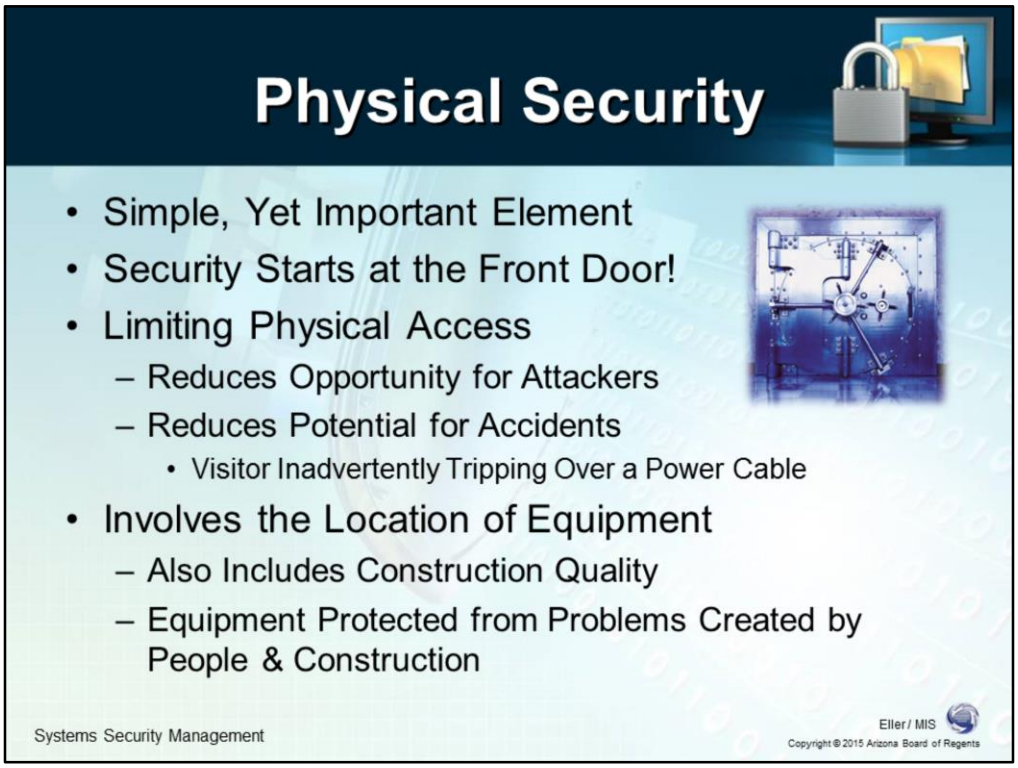

Physical & Network Security
Module 12
Systems Security Management
Eller / MIS
Copyright © 2015 Arizona Board of Regents



At the end of this module, you should be able to:

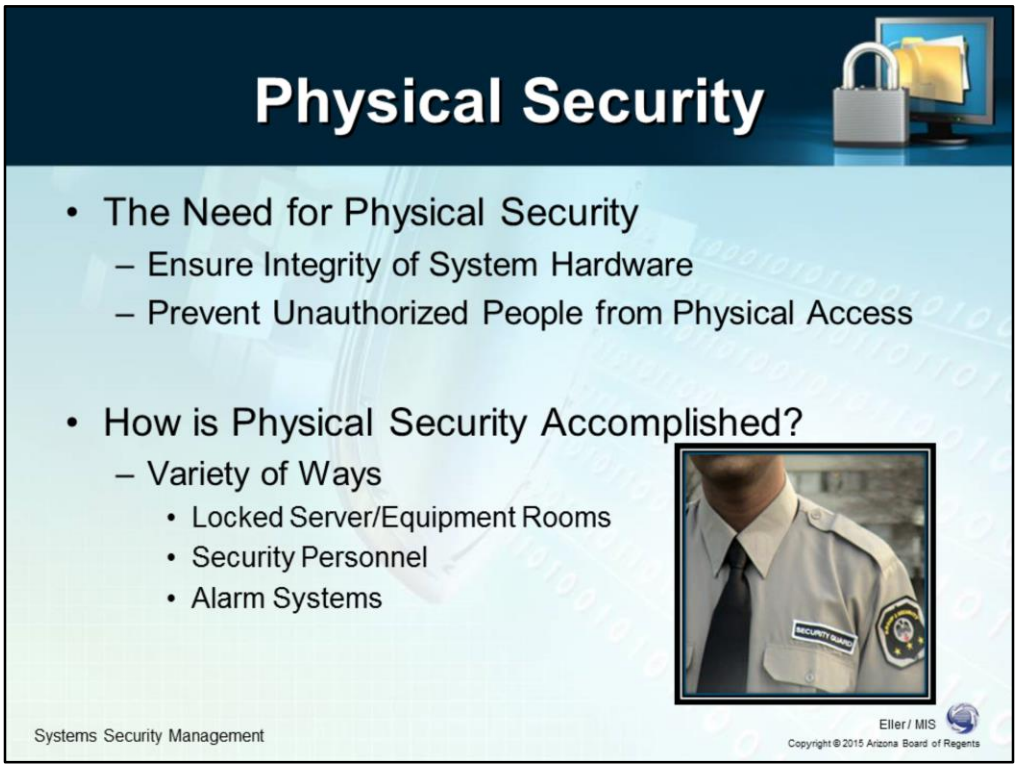
- Describe why physical security is just as important as system security.
- Describe how to physically secure workstations and servers.
- Describe the need for different facilities considerations such as HVAC, Power, and Fire Suppression.
- Describe the physical security concerns for media.
- Understand the need for fax security in organizations.
- Describe the different network topologies and understand how to design a network topology for security.
- Describe the differences between communications cabling and how secure each option is.
- Understand the accepted guidelines for cable installations.
- Understanding the implementation of structured network and wiring designs.
- Understand the need for virtual LANs and redundancy for security.
- Understand how aggregation is used to help improve network security.
- Describe the OSI model and its implications for network security.



Physical Security

Physical security is a very simple and important element to system security. Remember, security starts at the front door! Limiting physical access to resources is vital as it will reduce the opportunity for attackers to find a way to breach systems. In addition, physical security reduces the potential for accidents, such as a visitor inadvertently tripping over a power cable, causing a server to go offline in an unsafe manner.

Physical security involves the location of equipment and the construction quality within a building (or complex) with the end goal involving the protection of equipment from problems that are created by both people and construction.



Physical Security (continued)

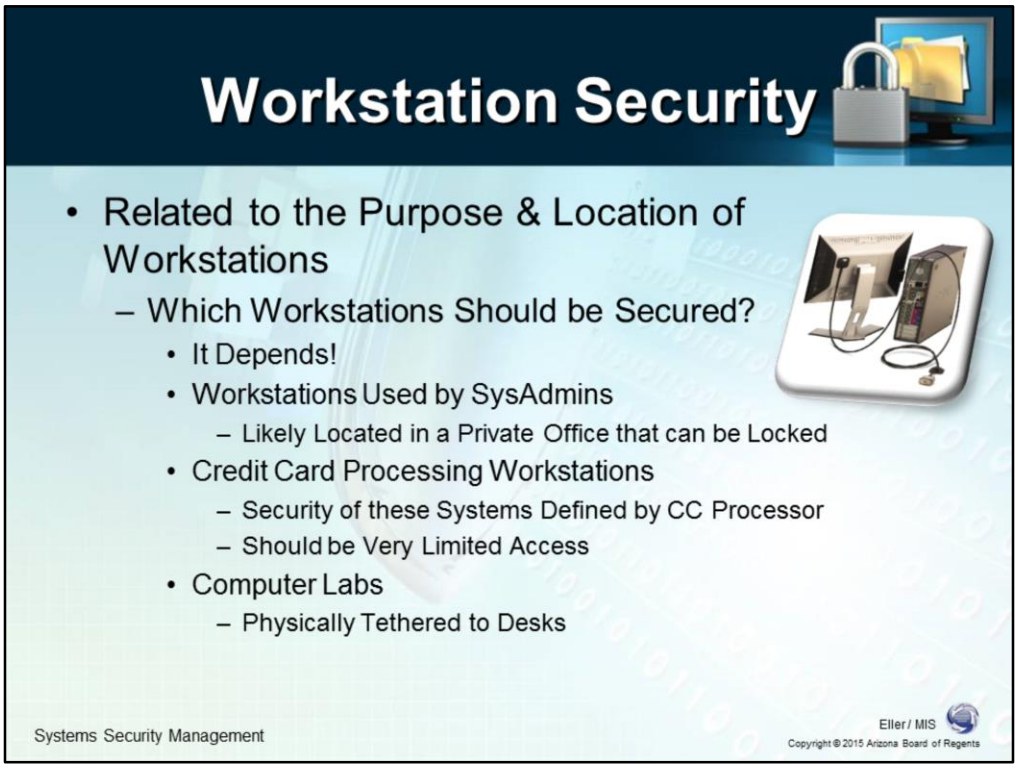
Physical security is necessary in order to ensure the integrity of system hardware by preventing unauthorized people from physical access. So, how is physical security accomplished? Well, there are a variety of ways in which to ensure the physical security of your systems, and many organizations use more than one of these options in order to provide a greater degree of physical security. Some of these security methods include locked server or equipment rooms, hiring security personnel, or implementing alarm systems.

Physical Security (continued)

Locked Server/Equipment Rooms – This should be a no brainer. In any organization, servers, especially those storing sensitive information, should be housed in locked server or equipment rooms. Access to these rooms should be restricted to SysAdmins and anyone else the organization deems should have access. These rooms can be locked with a variety of methods, including the standard lock and key, some kind of omnilock where a code is entered, a swipe system using ID badges, or even biometrics if necessary. Keeping systems locked in a specific room reduces the risk of unauthorized access and someone causing accidental damage.

Security Personnel – Some organizations choose to adopt the use of security personnel in order to ensure systems remain secure. Usually this involves having one or more security personnel on duty at any one time, monitoring the area using video cameras and periodic walkthroughs. Some also use security personnel to check ID badges to make certain only those who are authorized to be there are allowed in.

Alarm Systems – Alarm systems can also be installed in order to require those who need to access a locked system room to input a code in order to disable the alarm temporarily. These systems are a reasonable solution for maintaining security during times when access should not be necessary. For example, some organizations may only need to grant access to the system room during normal business hours, unless there is a system problem that requires access at other times. An alarm system can help to keep the system secure by notifying the authorities and the SysAdmin in the event the room is breached. Cameras can also be used to record video of the secured room itself and the entry ways in order to have a visual record in the event an alarm is tripped.



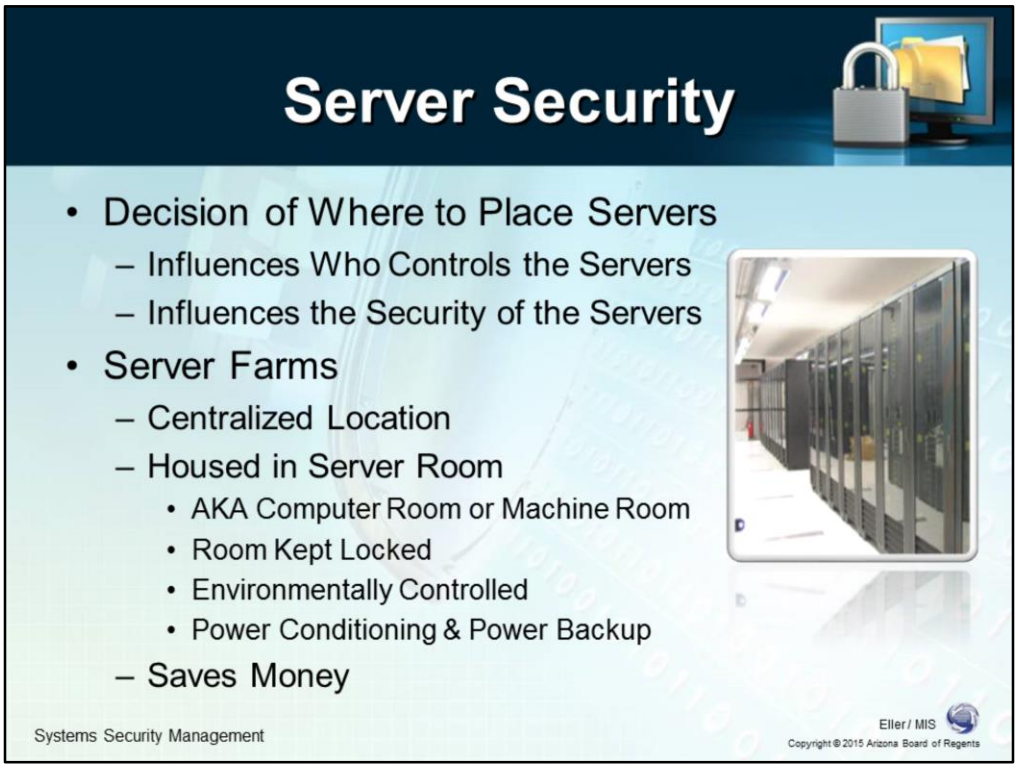
Workstation Security

The physical security of workstations should be related to the purpose and location of the workstations themselves. When evaluating an organization's resources, the question of which workstation to secure is not necessarily an easy question to answer. In general, any workstation that is used by a SysAdmin should be housed in a private office that can be locked. This is due to the nature of the tools installed on the workstation and the access rights that are necessary to manage the network. Credit card processing workstations should also be secured. The security of these systems is defined by the credit card processor, as there are a great number of requirements the organization will need to follow in order to ensure credit card information is handled securely. Because of this, a credit card workstation should have very limited access. Finally, another example involves publically accessible computer labs. Due to the nature of these systems being available to anyone who has access, they should be physically tethered to the desks in order to reduce the potential for theft.

Workstation Security (continued)

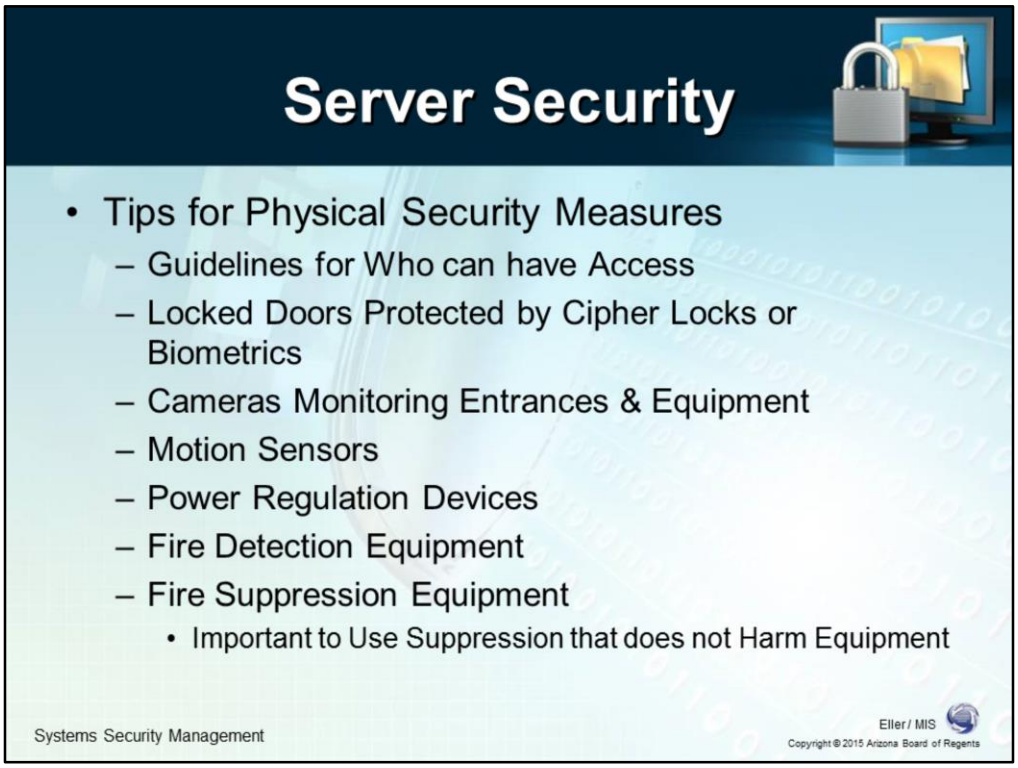
With workstation security, the training of users is vital to ensuring system security. Increasing awareness of the threats that exist is one of the best ways to counter those threats. Also, the physical aspect of locking doors and tethering systems are very obvious ways to secure systems, but also often ignored for convenience sake.

Another important workstation security method is preventing potential damage to workstations. With servers, they are generally housed in special areas with adequate ventilation and low risk of accidents. Workstations are generally out in the open and exposed to people, and people can have accidents. In general, to prevent damage, keep computer ventilation areas open to ensure adequate cooling. Keep the workstations away from the desktop edge so it cannot acidentally be knocked off the desk. Finally, keep workstations away from uncovered food or drinks. This last one is usually difficult, as we have all spent a lunch hour eating while working at our desks, but taking care to protect the workstation is not impossible.



Server Security

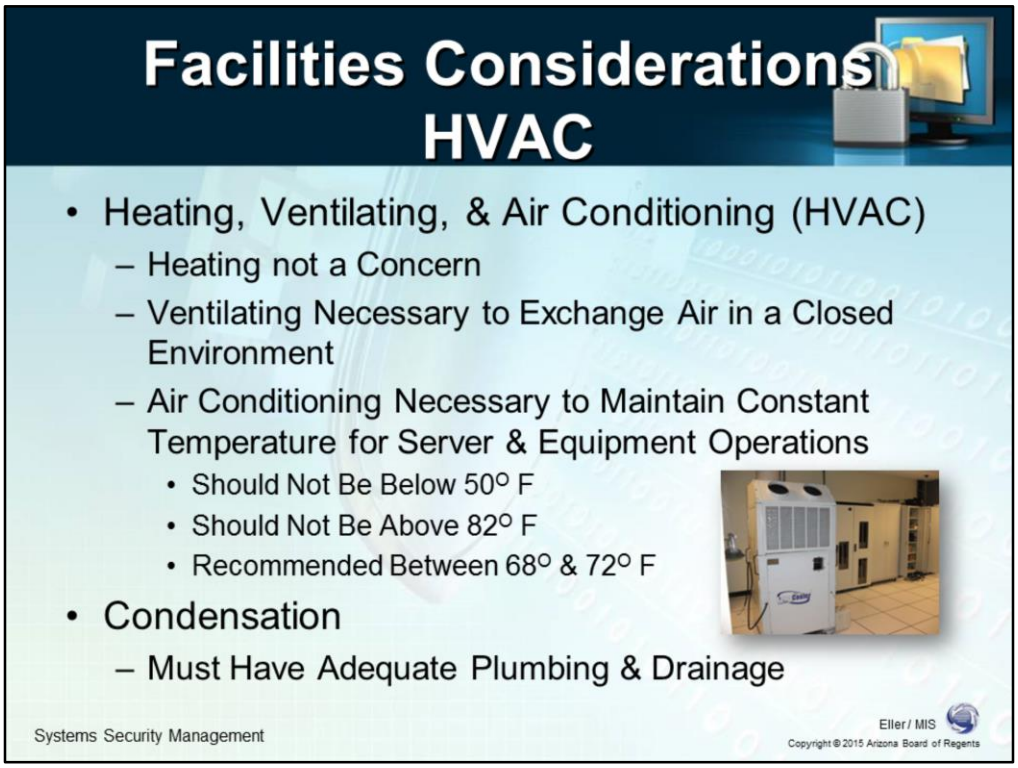
Physical security with respect to servers involves the decision of where to place the servers in a building. The placement of the server room influences who controls the servers and who influences the security of the servers. In general, servers farms, or large rooms filled with racks of servers, are generally placed in a centralized location and housed in a specialized server room. The server room should be kept locked at all times in order to prevent unauthorized people from entering. The room should also be environmentally controlled, with constant temperatures, power conditioning, and power backups. By consolidating into a single server room, this helps the organization save in overall operational costs.



Server Security (continued)

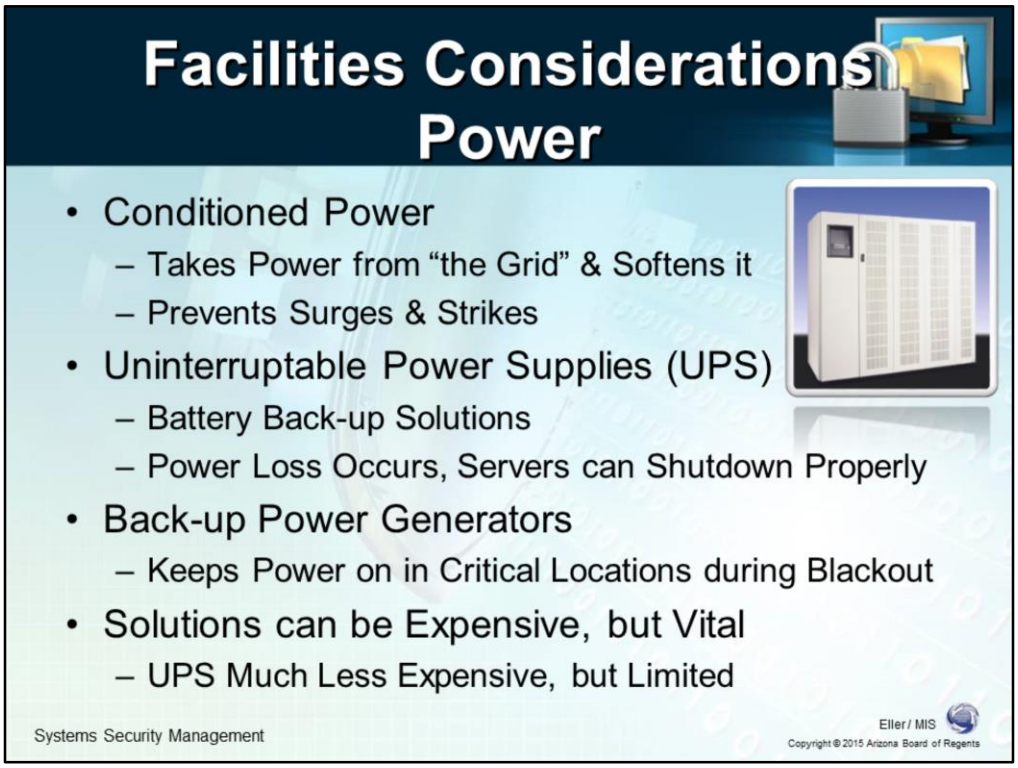
Depending on the organization and its individual need for security measures in the centralized server room, some of these physical security measures may or may not be excessive. The purpose here is to provide a variety of potential options for securing a server room.

Guidelines for Who can have Access – Organizations need to develop a series of guidelines, or official policies, that define who can and should have access to secured server rooms.
Locked Doors Protected by Cipher Locks or Biometrics – Server rooms need to be locked in order to prevent unauthorized access, and this is usually done with cipher locks or biometric devices. In a pinch, a normal lock and key can also be used, but this is a less secure option.
Cameras Monitoring Entrances & Equipment – In some cases it may be necessary to have video cameras used to monitor the entrances and exits of server rooms or inside the room itself. These videos will need to be monitored by someone within the organization, otherwise what is the point?
Motion Sensors – Motion sensors are also a technology which most may not find a need to deploy; however, motion sensors can be used to determine if someone has entered a secured area when no one is expected to need access.
Power Regulation Devices – Power regulation devices are used as a means to protect the equipment housed in the server room. Normal grid power fluctuates, which can cause severe damage to expensive equipment such as servers. Having a power regulation device will help to protect the servers from these fluctuations.
Fire Detection Equipment – Fire detection is a must. Fire can severely damage equipment and result in data loss, so being able to detect fires immediately is the key, which leads us into…
Fire Suppression Equipment – You definitely want to have some kind of fire suppression system in-place, keep in mind that it is important to use suppression that does not harm the equipment.



Facilities Considerations – HVAC

When looking into building the facilities for a server room, one of the most important areas to consider is environmental controls. In server rooms this means having dedicated heating, ventilating, and air conditioning, or HVAC, systems. These systems are designed to help maintain a very specific temperature and humidity level within the server room to allow the systems to run in optimal conditions. In general, heating is not a concern, the servers will generate plenty of heat on their own. Ventilation is necessary in order to exchange the air within the closed environment. Finally, air conditioning is necessary to maintain a constant temperature for operations. Temperatures should not be below 50 degrees Fahrenheit and should not be above 82 degrees Fahrenheit. The ideal temperature is a range between 68 and 72 degrees Fahrenheit. Because of this temperature requirement, the HVAC systems will generate a significant amount of condensation. It is important to ensure the server room has adequate plumbing and drainage available to prevent water damage.



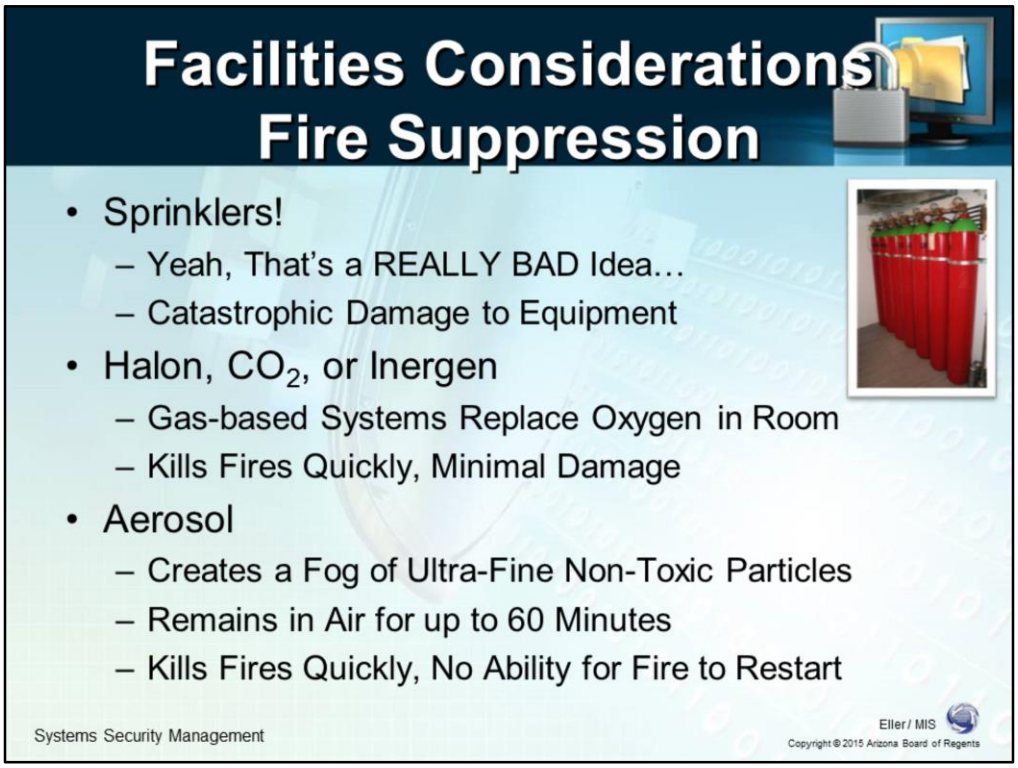
Facilities Considerations – Power

Another facility consideration should involve the power situation. Conditioned power solutions absolutely should be adopted for powering sensitive equipment. Conditioned power systems take their power directly from the "grid" and soften it. What this means is it takes power that can fluctuate and works to prevent any surges or spikes from making it to the servers and equipment.

Another option for power involves the use of uninterruptable power supplies (UPS). These are normally adopted as a battery backup solution, where if power is lost, the servers will continue to operate for as long as the batteries last. When evaluating the adoption of UPS systems, the SysAdmin must determine the amount of power necessary for the servers to continue operating for 15-20 minutes. This should be enough time to allow each server to be shut down properly and prevent data loss.

In the event it is necessary to never allow a power loss to prevent systems from running continuously, some organizations may need to install a back-up power generator. These are designed to kick in immediately when a power outage is detected, using UPS systems as a bridge while the generator starts up. This allows the organization to keep power on in critical locations during a local blackout.

In general, power solutions can be very expensive; however, depending on the organization, they may be vital to continued operations. Remember, a UPS system is a much less expensive solution, but it is limited in scope. If the need is greater than what can be achieved with a UPS, then a power conditioner or generator may be necessary.

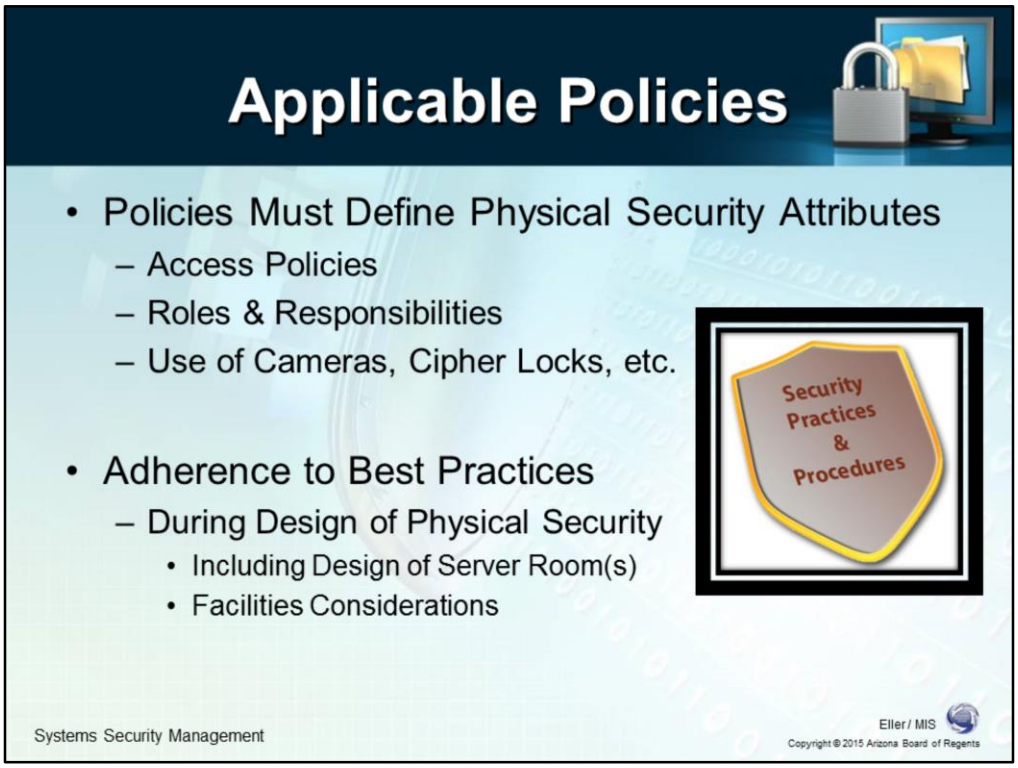


Facilities Considerations – Fire Suppression

Fires can cause severe damage to servers and other equipment, both from heat and the actual fire itself. This means it will be necessary to ensure there is a solid fire suppression system available to protect the systems from fire and heat damage. Now, the most important consideration here involves making sure the suppression solution that is used does not do damage to the equipment as well. So sprinklers? Yeah that is a really bad idea. Water will cause catastrophic damage to equipment.

Many organizations adopt the use of a halon, CO_2, or Inergen gas-based solutions as these are designed to replace the oxygen in the room with the respective gas. As we all know, fires require oxygen in order to burn, so replacing the oxygen with other gasses will choke the fire and force it to die out quickly. These result in minimal damage due to the fire; however, because of the nature of replacing the oxygen in the air, these solutions are fatally toxic to humans. These systems should not be deployed when someone is in the room, otherwise the person will suffocate as the oxygen is removed from the room. These solutions require some kind of monitoring system to prevent this type of event from occurring.

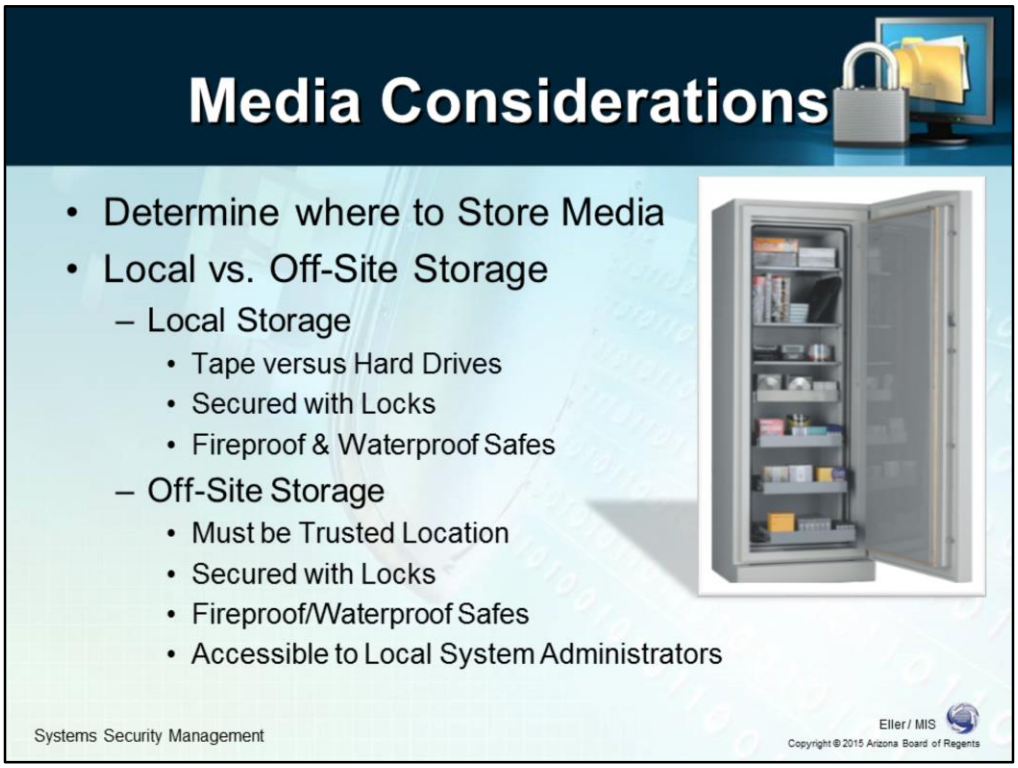
The most recent type of suppression system that is gaining popularity is an aerosol-based system. Aerosol systems create a fog of ultra-fine, non-toxic particles in the air that can kill a fire quickly. The aerosol also remains in the air for up to 60 minutes, preventing the fire from being able to restart if it is not completely out. These systems are able to be used even if someone is in the room as it is non-toxic.



Applicable Policies

As we have discussed in module 4's organizational security lecture, policies created by the organization need to take into account physical security attributes. These policies can include access policies, including who should have access to specific secure rooms, the roles and responsibilities of those who need to protect the resources, and the possible use of other security options, such as cameras and cipher locks, among others.

Organizations also need to adhere to best practices during the physical security design process. This should include the design of the server room(s) and facilities considerations.



Media Considerations

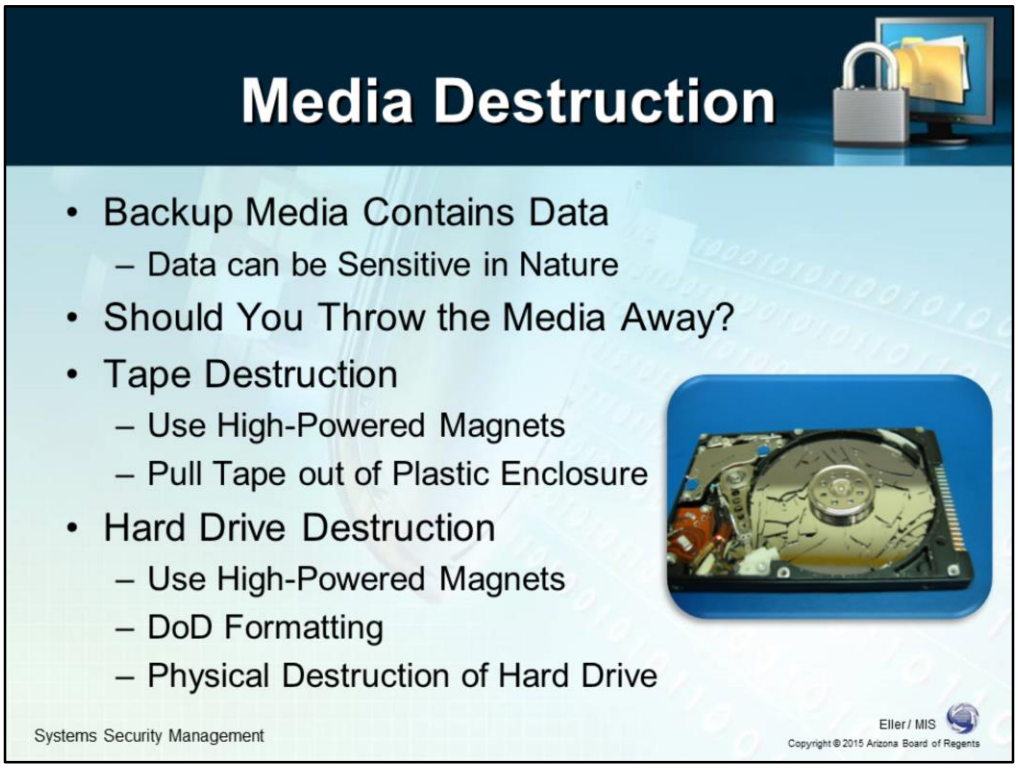
We have spoken before about backup media and the physical security of backup media is very important to consider. Where should an organization store its backup media when not in-use? The decision breaks down to local versus off-site storage.

Local Storage

With local storage, the SysAdmin needs to determine what type of media to use. The common media types include tapes and hard drives. When not in-use, whichever media type is selected should secured with locks. The reason is simple: the media contains copies of everything on your servers. If you store sensitive information on the servers, then the same security considerations for the backup media must be observed. The use of fireproof and waterproof safes are ideal for storing media locally.

Off-Site Storage

Backup media stored off-site needs to be stored in a trusted location. If the organization contracts with a third party for off-site storage, the contracts need to detail how the media will be stored and secured, how media is transported back and forth to the server location, and who has access to the facility, as well as what background checks have been performed on the employees. The off-site location should be secured with locks, possibly using fireproof and waterproof safes, similar to the local storage solution. In addition, the off-site location should be accessible in some way to the organization's SysAdmin.

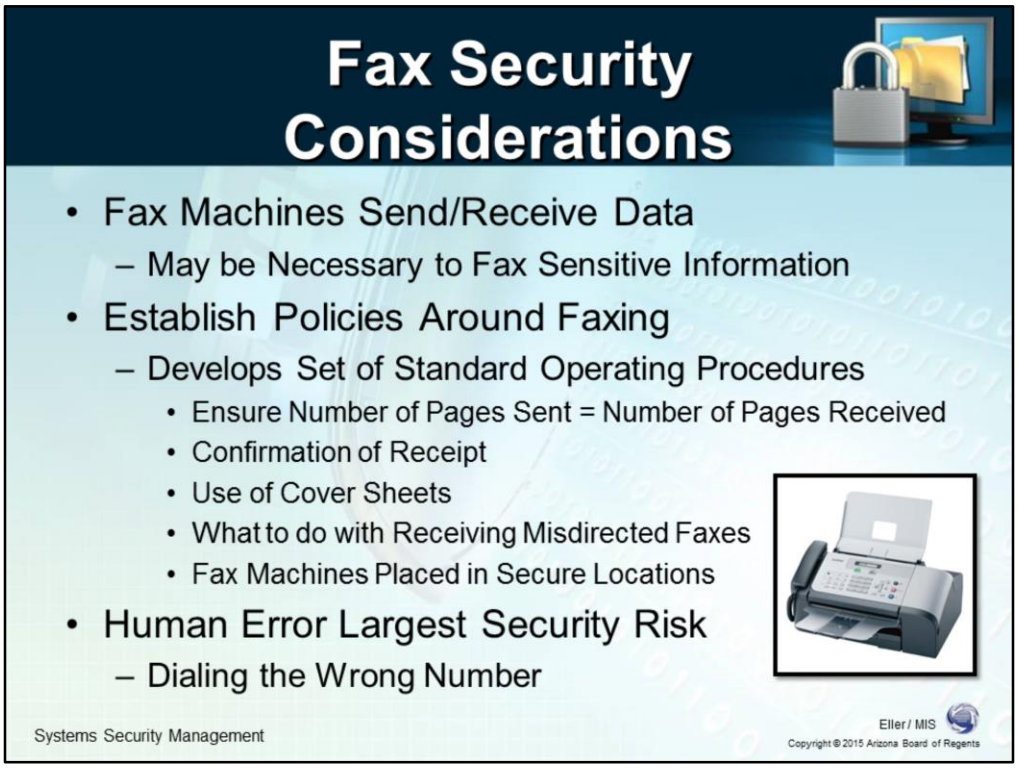


Media Destruction

The second part to physically securing backup media involves the destruction of the media. Going back to what was previously mentioned, backup media will contain the same information as is stored on the servers, which can include sensitive information. Taking this media and throwing it away does nothing to protect the data from being stolen. Only completely destroying the media will ensure the data is not recoverable. Depending on the media will determine how it should be destroyed.

Tapes can be destroyed in several ways. Since tapes are a type of magnetic media, you can use a high-powered magnet to erase the data contained on tapes. Alternatively you can pull the tape out of the plastic enclosure; however, just pulling it out will not be enough as it can easily be repaired and put back into another plastic enclosure to be read. The tape, however, can be melted in order to prevent this from happening.

Hard drives are also magnetic media, and as such they are also able to be erased using high-powered magnets. Another option for destroying the data on hard drives is to perform a DoD level format, which is designed to write random bits (ones and zeros) to every sector of the hard drive a minimum of seven times in order to make data unrecoverable. The final method would be to completely destroy the hard drive by crushing it or shattering the platters.



Fax Security Considerations

Fax machines have been around for decades. How many of you have thought about the security of the information you are sending to someone via fax? Have you ever had to fill out a standard form that you needed to fax to someone for processing that contained your name, address, phone number, and possibly even your social security number or credit card numbers? What is to guarantee that the person on the receiving end of the fax is standing next to the machine ready to take the pages as they print out? This is a major security issue that many do not consider unless there is precedent or is something the organization takes into account.

In order to protect information that is faxed, organizations must establish policies around faxing. Developing a set of standard operating procedures for sending and receiving faxes is important. Here are some areas to consider:

Ensure Number of Pages Sent = Number of Pages Received – If there are pages missing, then either someone took a page accidentally with a previous fax or the fax may have been intercepted during communication and modified.
Confirmation of Receipt – Once a fax has been received the sender should expect to receive some kind of confirmation the fax was received, either through a phone call, e-mail, or fax-back.
Use of Cover Sheets – Cover sheets protect the contents of your fax by printing a sheet that comes before the necessary data. The cover sheet should include important information such as who the fax is from, who is the receiving party, callback phone number for confirmation, and the number of pages in the fax.
What to do with Receiving Misdirected Faxes – If you receive a fax from someone unexpected, or containing information clearly not intended for you, how do you handle this? Do you call the person if they included a cover sheet? Do you destroy the fax?
Fax Machines Placed in Secure Locations – Fax machines used for receiving sensitive information should be kept in a secured location in order to protect faxes that come in when the receiving party is not available.

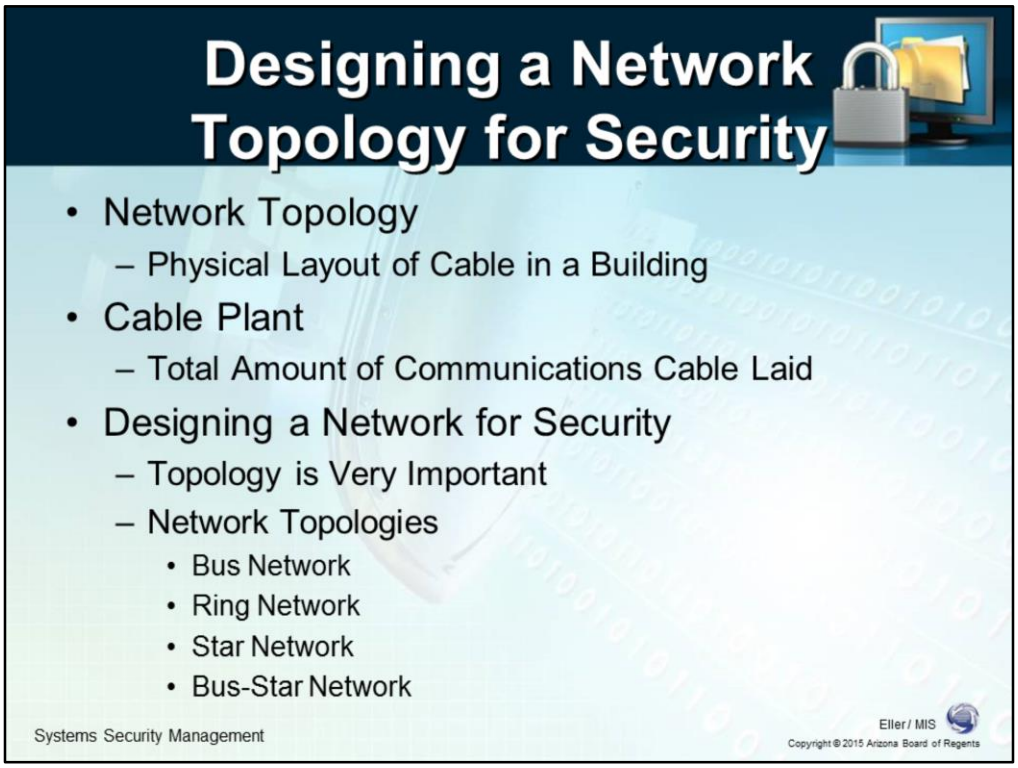
The most important thing to realize is human error is the greatest security risk when it comes to faxing. People can very easily dial an incorrect number and send the fax to the wrong location, so it is important to follow up immediately after sending a fax to ensure it was received at the intended destination.

Zone Control

As we have discussed, controlling access to secure locations is an important part of the physical security puzzle. Zone controls in physical security involves the defining of the roles and responsibilities for personnel who have physical access to secure areas. In some cases it may be advisable to provide physical access during only specific times of the day. Perhaps there is a need for three shifts of SysAdmins and each shift should only have access during their specific shift, give or take a few hours in either direction.

Another zone control for physical security is achieved by centralizing the server farms. Keeping all servers in a central location will minimize the physical area that needs to be secured, reducing some of the costs of operations and physical security. In addition, it may be necessary to decentralize the network communications closets. This will depend on the size of the building and if the building has more than one floor. In these instances, decentralizing the network closets is absolutely necessary. These closets should be secured with locks, and the keys and access rights should be tightly controlled.

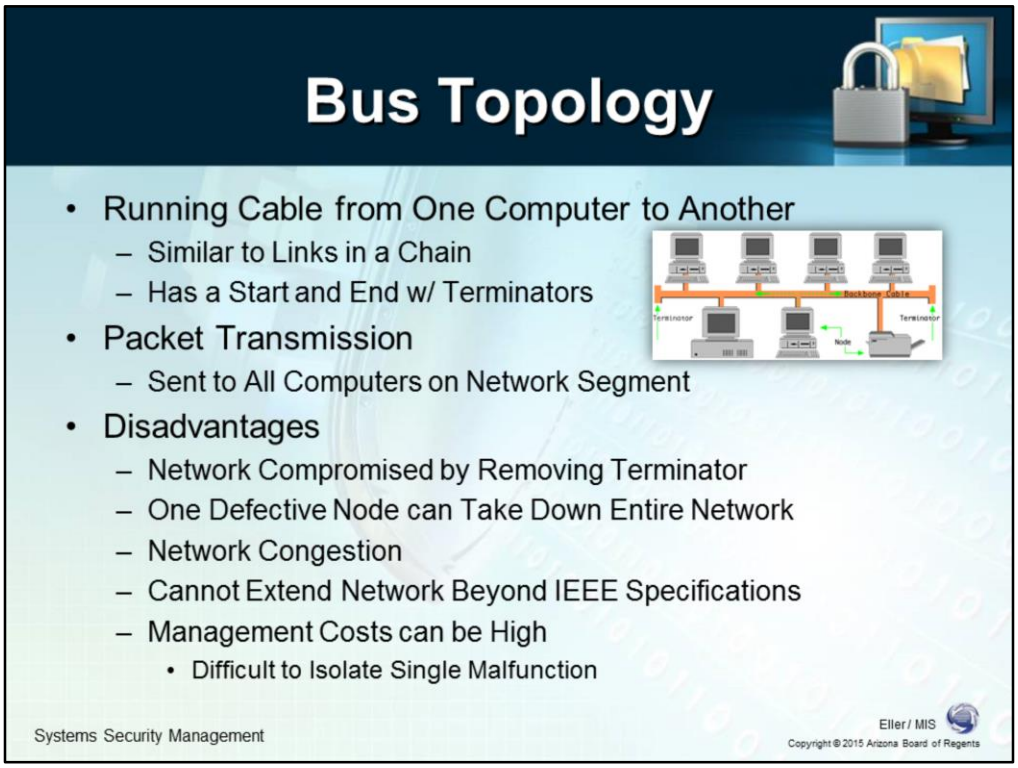
The ability to monitor/control access in a central location should be considered critical in an enterprise environment. The use of digital key cards and/or biometrics are essential, but the ability to monitor who goes where and when, along with a system to provide intelligent analytics on that information is key to spotting and warning administrators that untoward activity may be occurring. Janitorial staff are often granted access to places that contain highly sensitive material in order to do their jobs; having the system know that someone is accessing an area outside their normally scheduled time, as well as in a different location than they are usually assigned - and then sending an alert - can mean stopping a data breach or exfiltration before it happens.



Designing a Network Topology for Security

Going hand-in-hand with physical security is the physical design of the network so it incorporates strong security elements. When designing a network, it is necessary to adopt a network topology, which is the physical layout of network cable in a building. In terms of the cable itself, the total amount of communications cable laid within a floor or building is referred to as a cable plant.

Designing a network for security means adopting the network topology which best suits the needs of the organization. It is extremely important to pick an appropriate topology, as that will determine the equipment that will be necessary and the types of security options that will be available. The different network topologies include: bus, ring, star, and bus-star networks.



Bus Topology

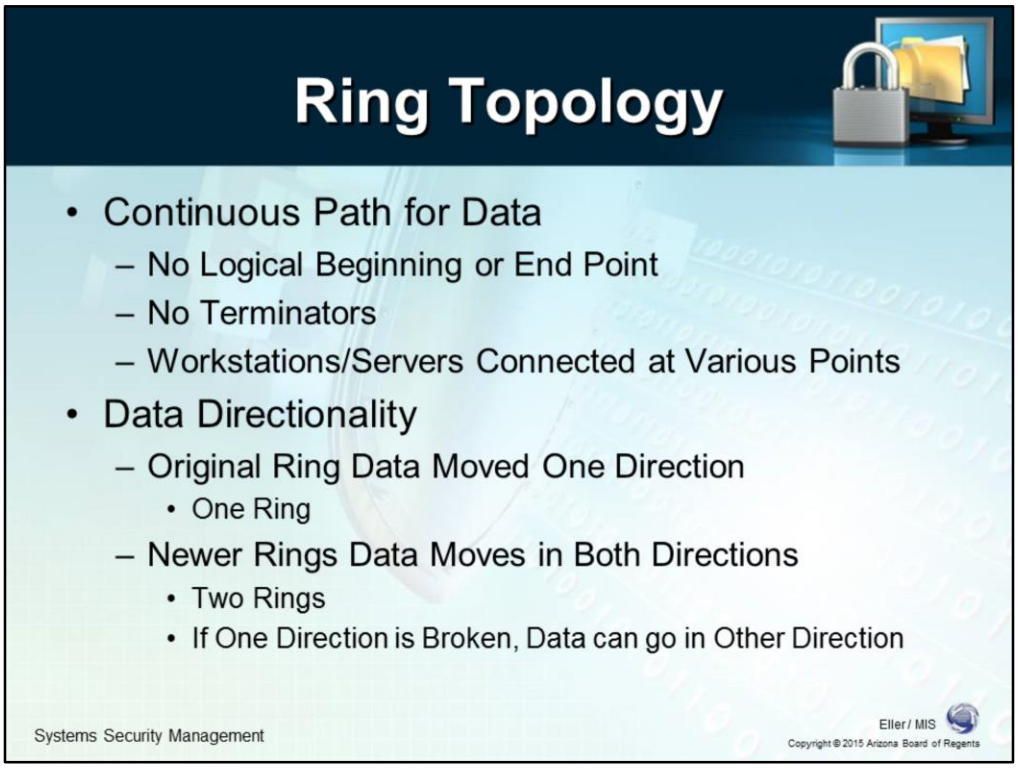
Bus topology uses a common backbone to connect all the network devices in a linear shape. A single cable functions as the shared communication medium for all the devices attached to this cable with an interface connector. In this regard, the bus is very similar to the links in a chain. One important piece to understand is the network must have a device at either end of the cable called a terminator. Terminators are used to signify the start and end of a network segment.

In addition, the device, which wants to communicate sends the broadcast message to all the devices attached with the shared cable, but only the intended recipient actually accepts and processes that message. Ethernet bus topologies are easy to install and don't require much cabling, only a main shared cable is used for network communication.

Disadvantages

Bus networks are very easy to disrupt. The network will become compromised if a terminator malfunctions or is removed from the cable. In addition, if a single computer node is defective, it can take down an entire network, similar to how older style Christmas lights worked (if one bulb burned out, the entire strand would not light up).

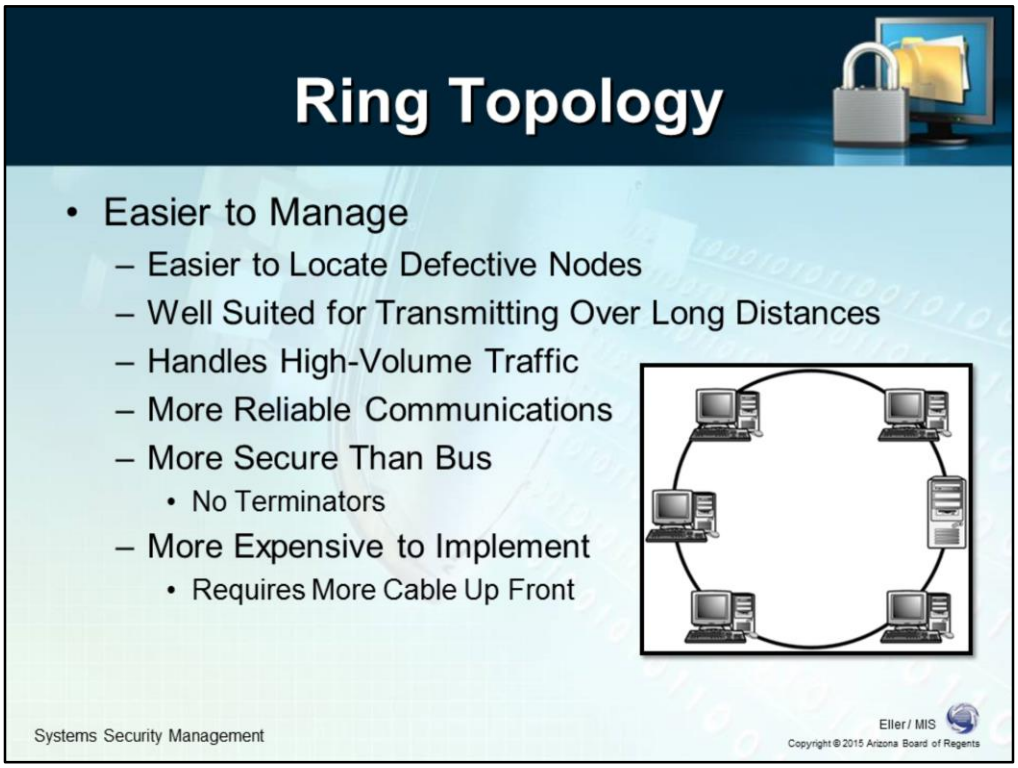
Performance issues are likely to occur in the Bus topology if more than 12-15 computers are added, as the extra computers will increase the amount of network chatter, causing congestion. Additionally, if the Backbone cable fails then the network becomes useless and communication fails among all the computers. For all of these reasons, a bus network cannot extend beyond the IEEE specifications. Due to the nature of how a bus network is configured, the management costs can be high, and it can be very difficult to isolate a single station that is malfunctioning (Overview of Computer Network Topologies, 2007).



Ring Topology

A ring topology is designed as a continuous path for data transmissions. Every computer attached to the network has two adjacent neighbors for communication. This means there is no logical beginning or end point to the network, and because of this no terminators are necessary. Workstations and servers are connected at various points around the ring.

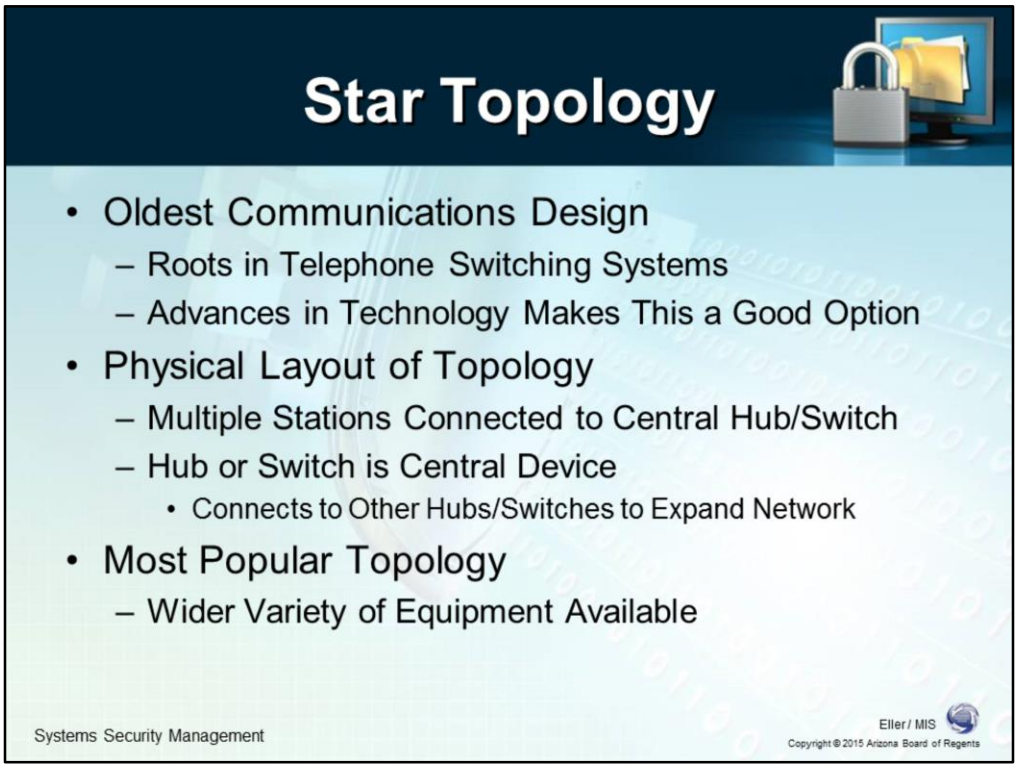
When it comes to data transmission, the original version of the ring topology allowed data to move in a single direction (or a one ring network). For lack of a better description, this means if the data moves along the network to the right, the data will go to each computer on the ring until it arrives at its final destination. So, many computers on the network will receive the data and forward it to the next node. Newer ring networks move the data in two directions (a double ring), allowing for shorter transmission times and redundancy in the event one of the rings were to fail (Overview of Computer Network Topologies, 2007).



Ring Topology (continued)

A ring network is much easier to manage than a bus network. For starters it is easier to locate defective nodes on the network, especially since the ring network allows for defective nodes to be bypassed, resulting in a network that continues to function properly. Ring networks are well suited for transmitting over long distances due to the cable and equipment used. In addition, the ring handles high-volume traffic more efficiently, reducing network congestion when additional nodes are added, resulting in more reliable communications.

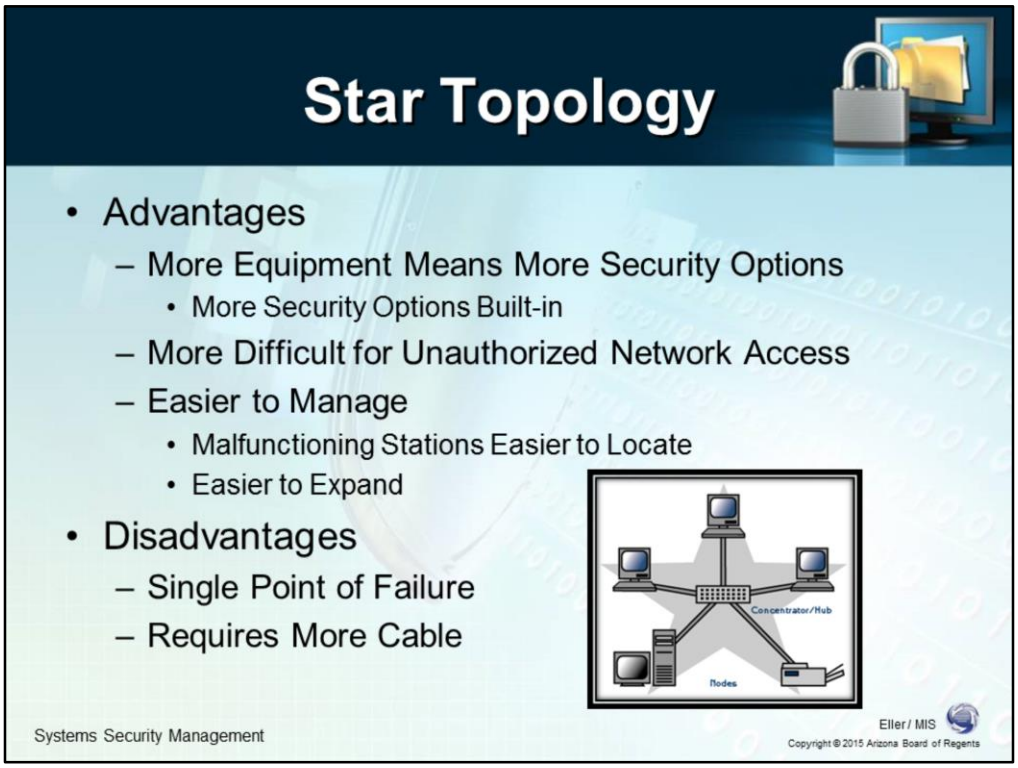
Since a ring network does not require the use of terminators, it is more secure than a bus network since there can be no network disruption due to a terminator being removed. The caveat of this network topology is it is very expensive to implement as it requires significantly more cable and equipment than other topologies. The ring topology has become almost obsolete (Overview of Computer Network Topologies, 2007).



Star Topology

The star network topology is the oldest communications design, with roots in telephone switching systems. In the computer world, the star topology is the most commonly used topology in LANs, and advances in technology make this a good option.

The physical layout of the star topology involves multiple stations that are connected to central devices like hubs, switches or routers. The hub or switch is a central device that connects to other hubs and switches in order to expand the network. Because of how easy it is to add new segments or nodes to the network, the star is the most popular topology. As such, there is a much wider variety of equipment available for this network type (Overview of Computer Network Topologies, 2007).



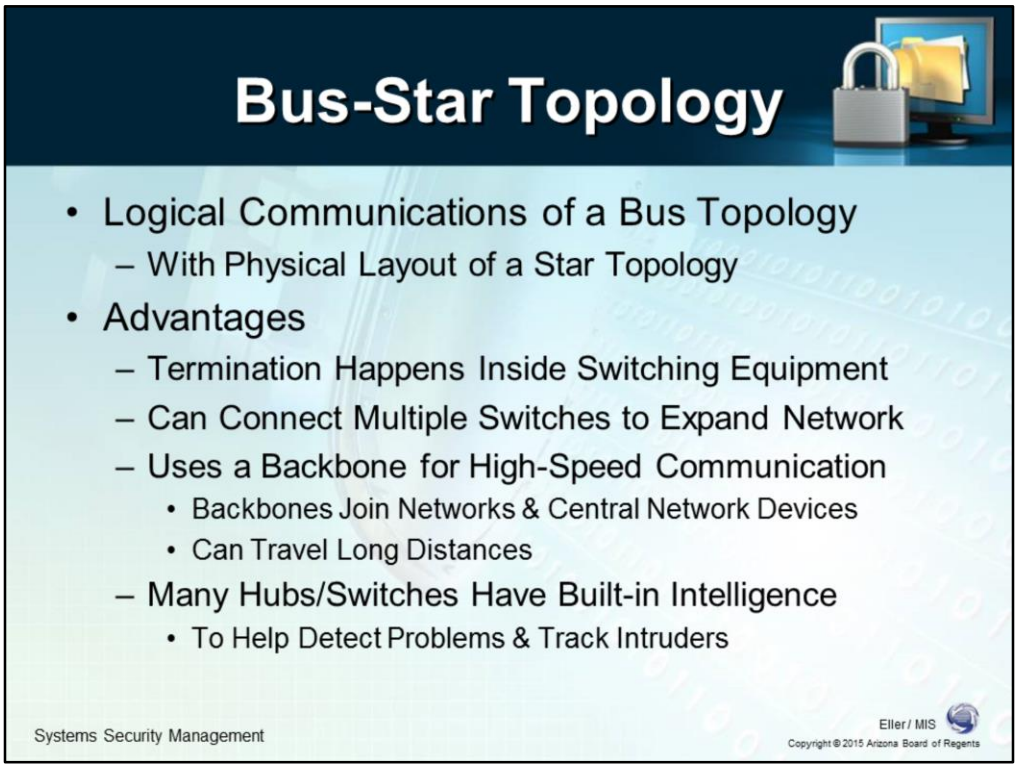
Star Topology (continued)

Advantages

There are many advantages to adopting a star topology. Since the topology is so popular, there is more equipment available for purchase, which means there are more security options available, many of which are built-in. The star network requires running a cable to each node location, making it more difficult for unauthorized network access to occur. Finally, the star topology is easier to manage when compared to other topologies. Malfunctioning stations are much easier to locate as you can unplug each node until you locate the defective one, and the network can be expanded with relative ease, just by adding a new hub or switch.

Disadvantages

Despite the many advantages, there remain a couple of disadvantages to this topology. The most important of which involves the very nature of the star topology: hubs and switches. If a single hub or switch fails, individual segments or even the entire network can go offline. Finally, the star topology requires much more cable to implement than that of a bus or ring network (Overview of Computer Network Topologies, 2007).

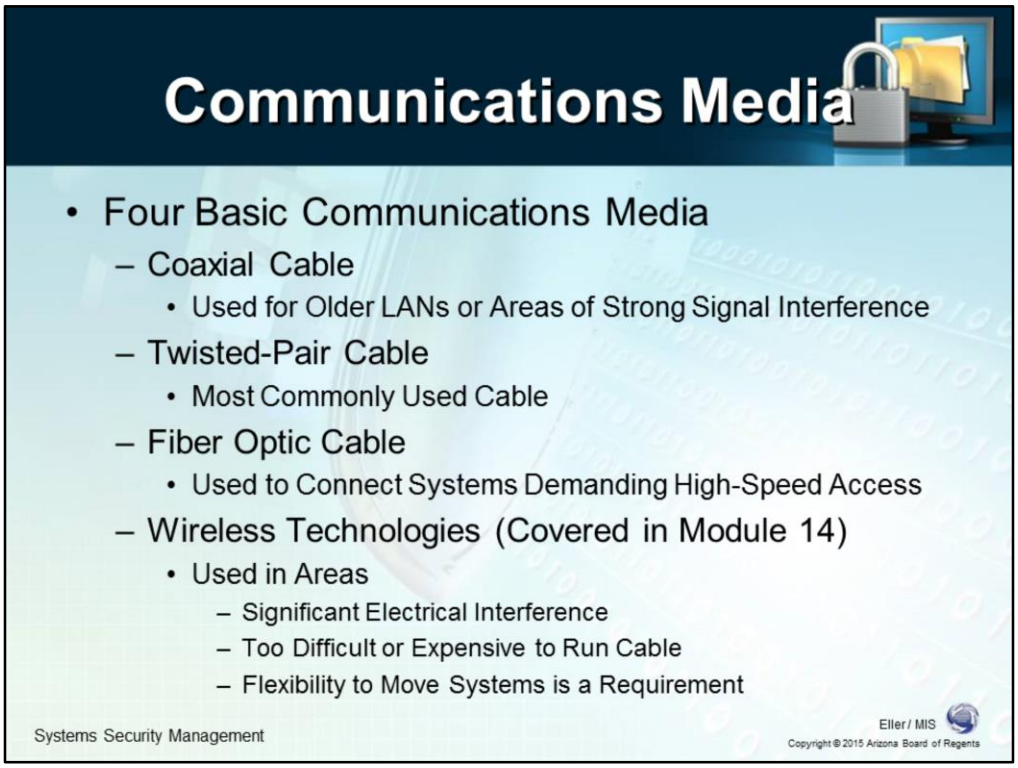


Bus-Star Topology

The Bus-Star topology takes the logical communications of a bus and combines it with the physical layout of a star topology.

Advantages

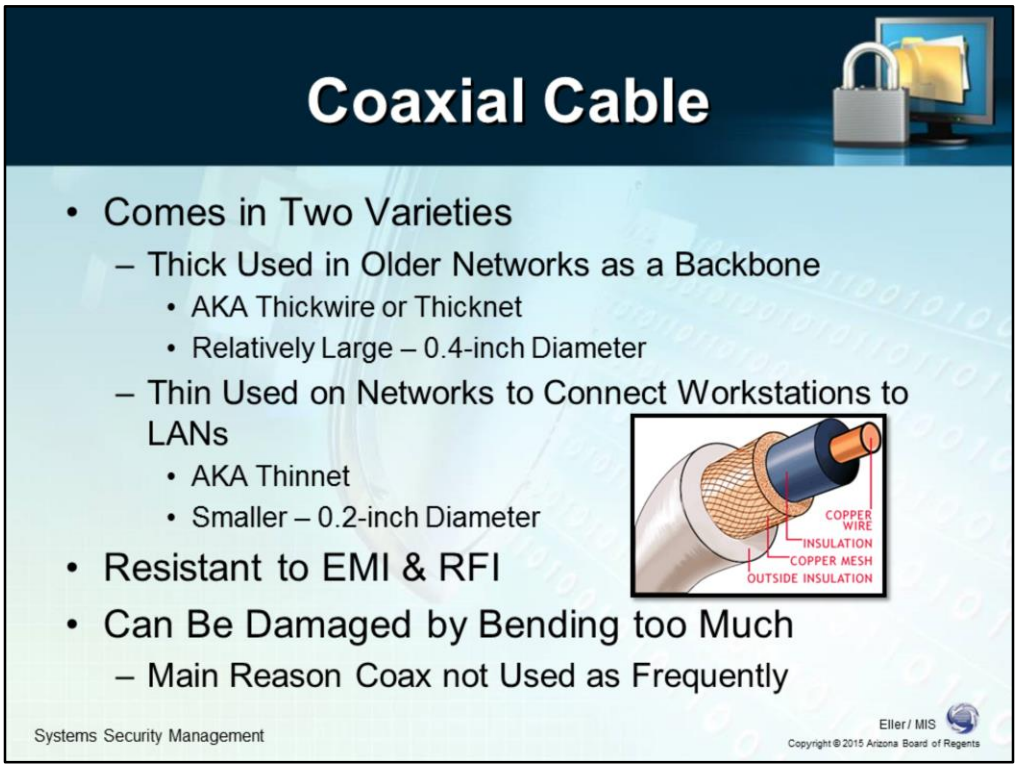
There are several advantages to using the bus-star topology. With this topology, the termination required for the logical bus occurs within the switching equipment. As with a star topology, you can easily connect multiple switches in order to expand the network. Another major benefit to a bus-star is that it utilizes a network backbone for high-speed communications. These backbones join networks and central network devices and can travel long distances. Finally, many of the hubs and switches used in a bus-star have built-in intelligence to help detect problems when they occur and track intruders.



Communications Media

In network telecommunications, there are four basic communications media:

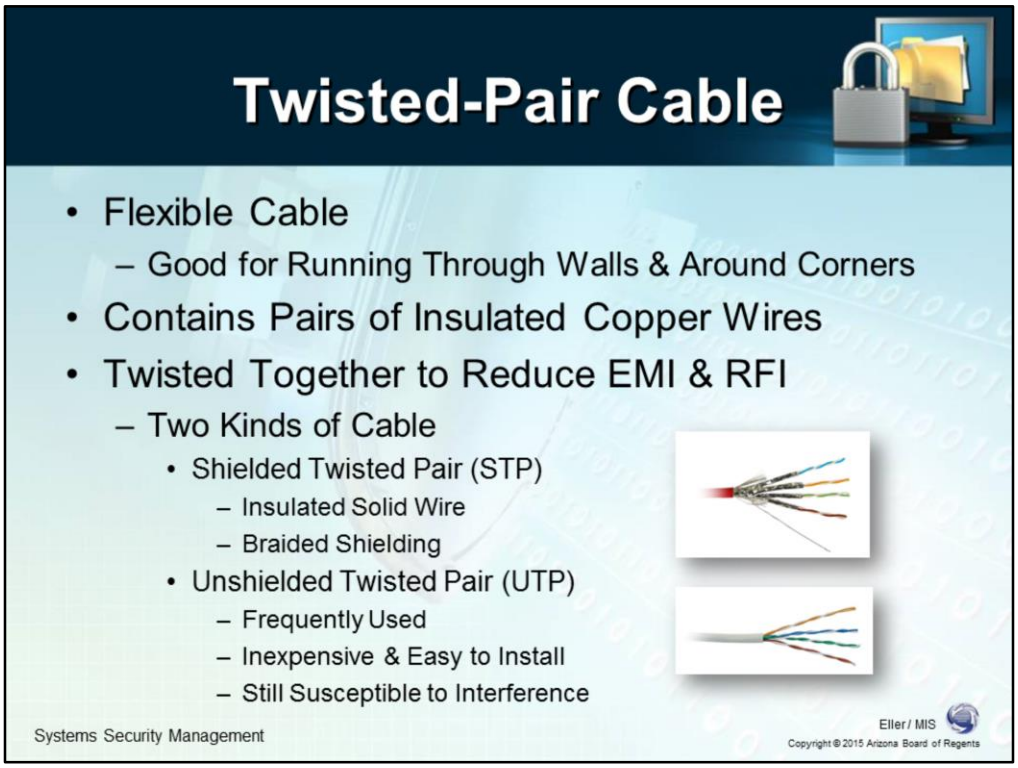
- **Coaxial Cable** – used in older LANs or areas of strong signal interference.
- **Twisted Pair Cable** – the most commonly used cable.
- **Fiber Optic Cable** – used to connect systems demanding high-speed access.
- **Wireless Technologies** – this is covered in Module 14; however, it is commonly used in areas where significant electrical interference exists, it is too difficult or expensive to run cable, and when the flexibility to move systems is a requirement.



Coaxial Cable

Coaxial Cable (or Coax) comes in two varieties: thick and thin. Thick coax cable is used in older networks as the network backbone. This type of cable is also referred to as thickwire or thicknet cable, and is relatively large with a 0.4 inch diameter. Thin Coax cable, or Thinnet cable, is typically used on networks to connect workstations to LANs. This cable is referred to as thin because it measures a 0.2 inch diameter.

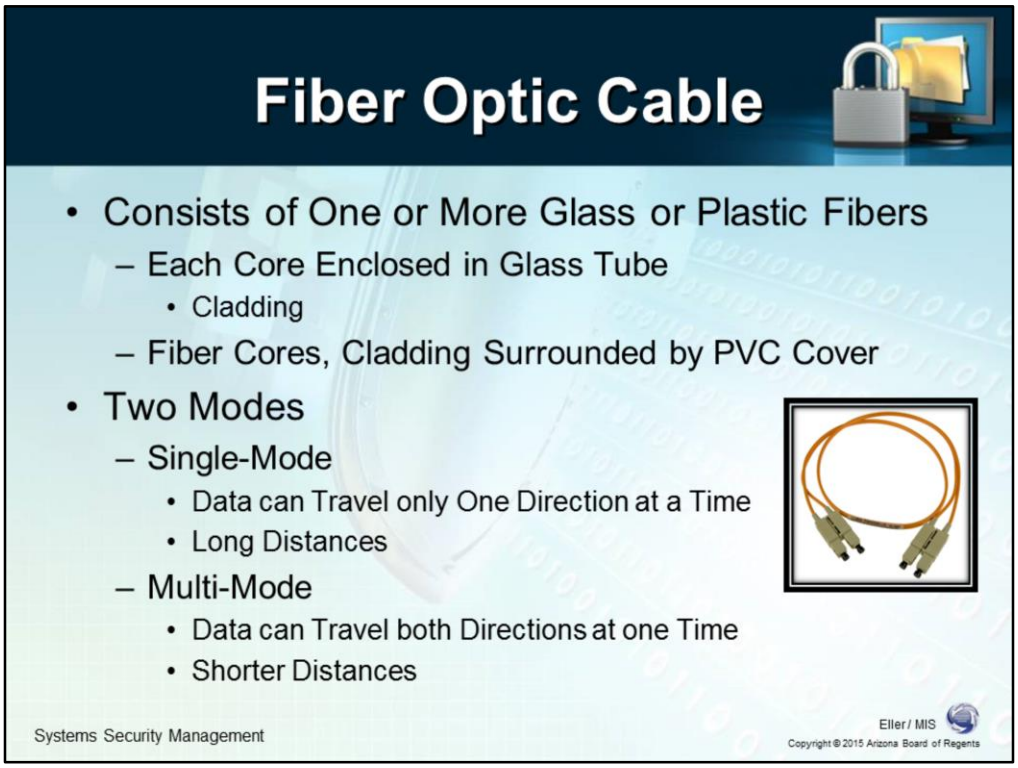
Coax cable is resistant to electromagnetic interference and radio frequency interference due to its construction. Coax cable consists of a solid copper wire surrounded by insulation. Around the insulation is a copper mesh which is then surrounded by an outer layer of insulation. One thing to keep in mind is despite the varying thickness of the cables, they can be damaged easily by bending them too much. This is the main reason why coax is not used as frequently on computer networks.



Twisted Pair Cable

Twisted pair cable is the most flexible network cable, making it great for running through walls and around corners. This cable contains pairs of insulated copper wires that are twisted together in order to reduce the potential for electromagnetic and radio frequency interference. There are two types of twisted pair cable: shielded and unshielded.

- **Shielded Twisted Pair (STP)** uses an insulated solid wire surrounded by a braided shielding.
- **Unshielded Twisted Pair (UTP)** is frequently used, inexpensive, and easy to install; however, due to the lack of shielding, this cable is still susceptible to interference.



Fiber Optic Cable

Fiber optic cable consists of one or more glass or plastic fibers, with each core enclosed in a glass tube, or cladding. The fiber cores and cladding is then surrounded by a PVC cover. There are two different modes of fiber optic cable: single-mode and multi-mode.

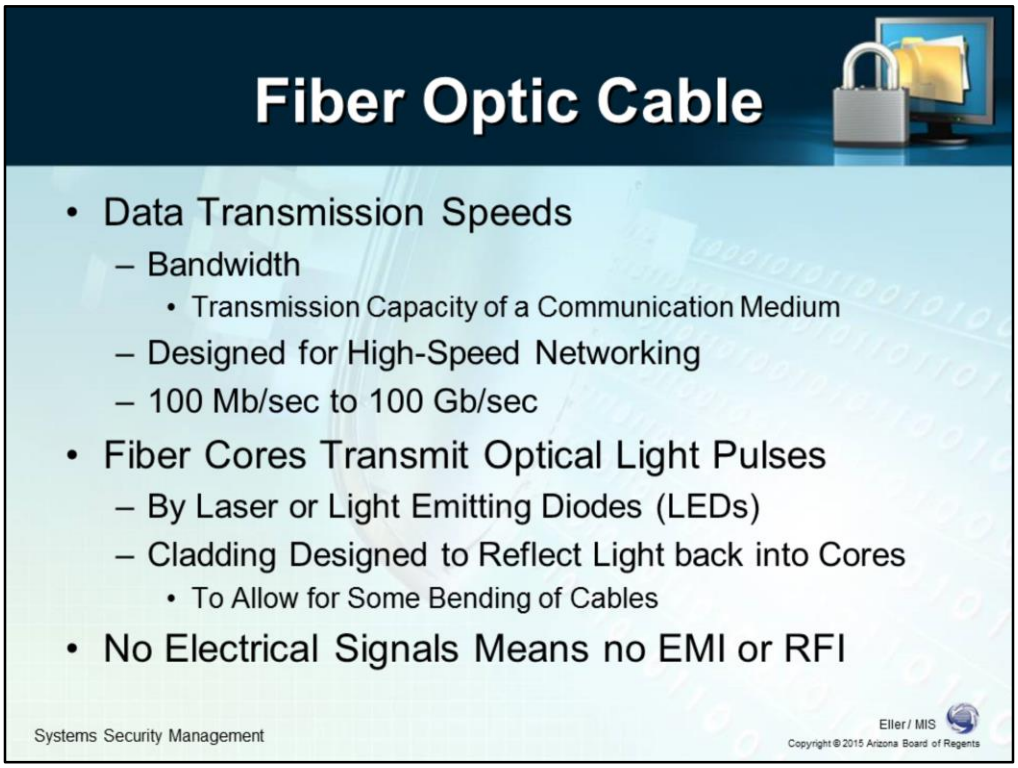
Single Mode Fiber is a single strand of glass fiber with a diameter of 8.3 to 10 microns that has one mode of transmission, typically 1310 or 1550nm. SMF carries higher bandwidth than Multi-Mode fiber, but requires a light source with a narrow spectral width.

Single-mode fiber gives you a higher transmission rate and up to 50 times more distance than Multi-Mode, but it also costs more. The small core and single light-wave virtually eliminate any distortion that could result from overlapping light pulses, providing the least signal attenuation, longest distance, and highest transmission speeds of any fiber cable type.

Multi-Mode cable is made of multiple glass fibers, with common diameters in the 50-to-100 micron range for the light carry component (the most common size is 62.5). POF is a newer plastic-based cable, which promises performance similar to glass cable on very short runs, but at a lower cost.

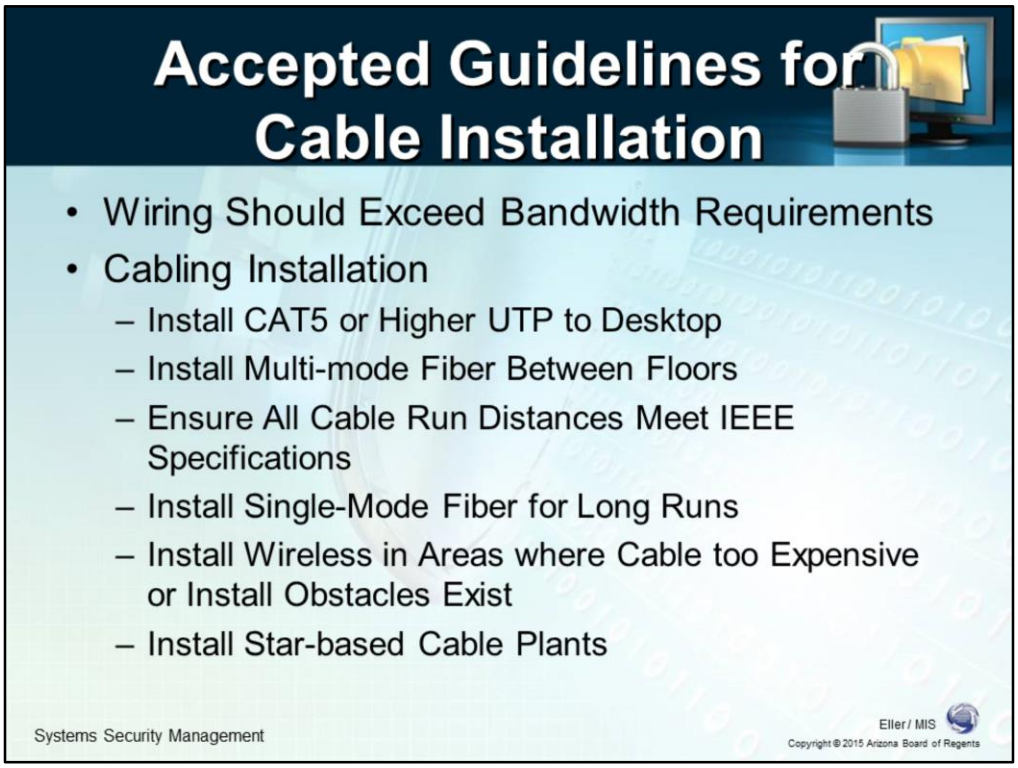
Multi-Mode fiber gives you high bandwidth at high speeds over medium distances. Light waves are dispersed into numerous paths, or modes, as they travel through the cable's core typically 850 or 1300nm. However, in long cable runs (greater than 3000 feet), multiple paths of light can cause signal distortion at the receiving end, resulting in an unclear and incomplete data transmission.

Due to the speed and length differences, Multi-Mode fiber is often used in general data and voice applications, such as bringing fiber to the desktop and adding segments to an existing network, while single-mode fiber is used for long-haul connections spread out over an extended area, such as campus backbone or television network applications.



Fiber Optic Cable (continued)

Data transmission speeds, or bandwidth, is the transmission capacity of a communication medium. Fiber optic cable was designed for high-speed networking, with speeds ranging from 100 megabits per second up to 100 gigabits per second or higher. This is because the fiber cores transmit optical light pulses via laser or light emitting diodes, or LEDs. The cladding is designed to reflect the light pulses back into the cores, so the light continues to transmit over the length of the cable. This cladding does allow for some bending of the cables. At no time during data transmission with fiber optics is an electronic signal used. This means there will be no electromagnetic or radio frequency interference.

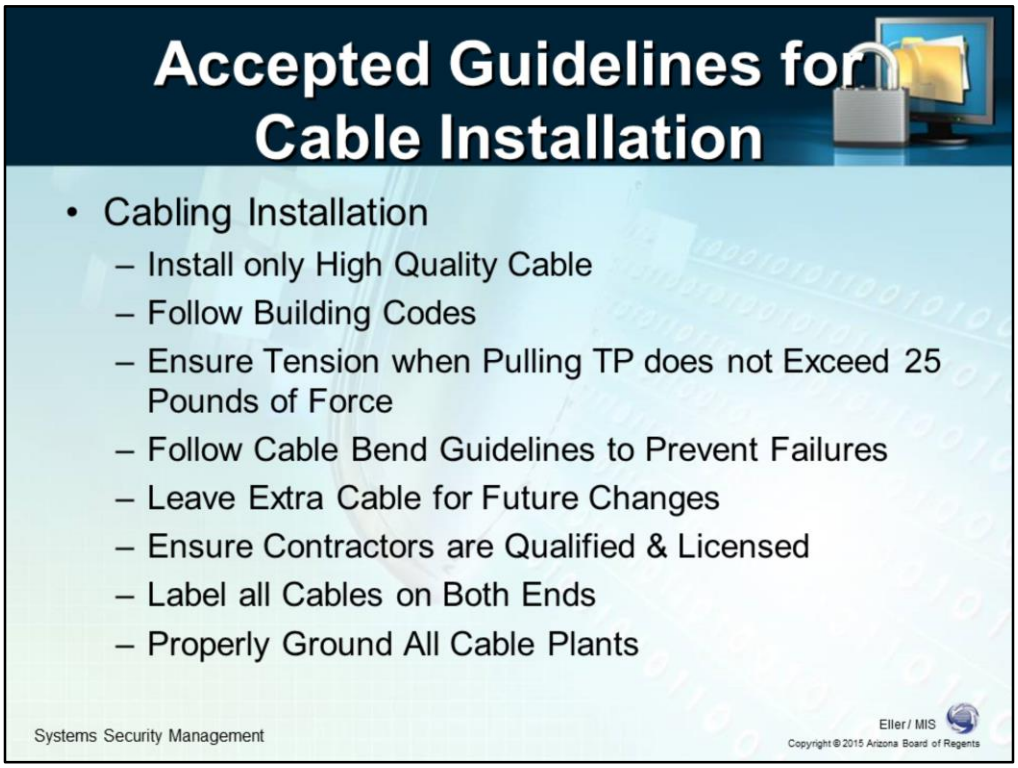


Accepted Guidelines for Cable Installation

Despite the topology you have adopted for your network, there are several generally accepted guidelines for cable installation. One important consideration is the wiring you choose to install should exceed the network's required bandwidth, otherwise you will find yourself with an underperforming network.

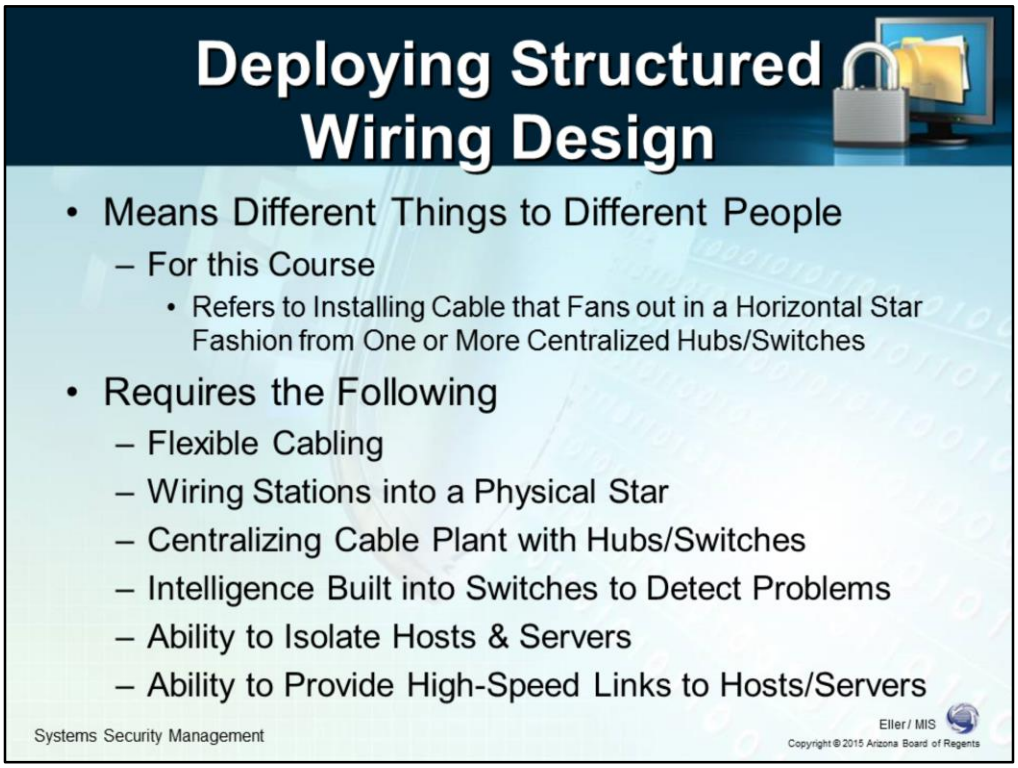
Cabling Installation

- Install CAT5 or Higher UTP to Desktop
- Install Multi-mode Fiber Between Floors
- Ensure All Cable Run Distances Meet IEEE Specifications
- Install Single-Mode Fiber for Long Runs
- Install Wireless in Areas where Cable too Expensive or Install Obstacles Exist
- Install Star-based Cable Plants



Accepted Guidelines for Cable Installation (continued)

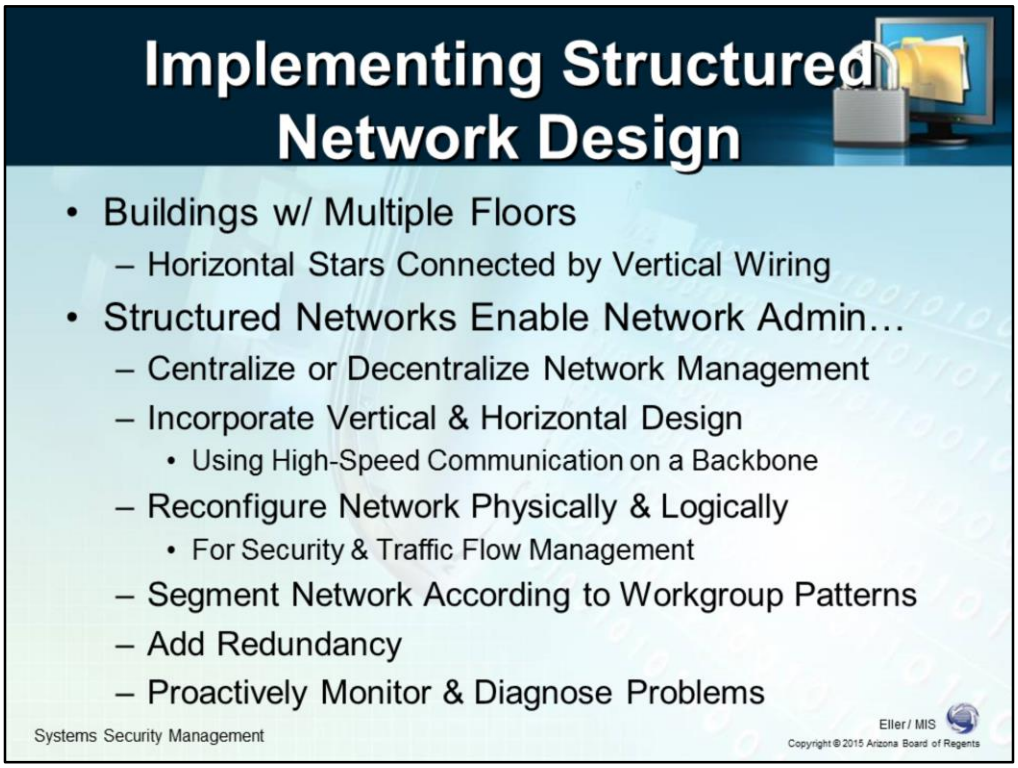
- Install only High Quality Cable
- Follow Building Codes
- Ensure Tension when Pulling TP does not Exceed 25 Pounds of Force
- Follow Cable Bend Guidelines to Prevent Failures
- Leave Extra Cable for Future Changes
- Ensure Contractors are Qualified & Licensed
- Label all Cables on Both Ends
- Properly Ground All Cable Plants



Deploying Structured Wiring Design

Deploying a structured wiring design means different things to different people. For the purposes of this course, this refers to installing cable that fans out in a horizontal star fashion from one or more centralized hubs or switches. In order to accomplish this it requires the following:

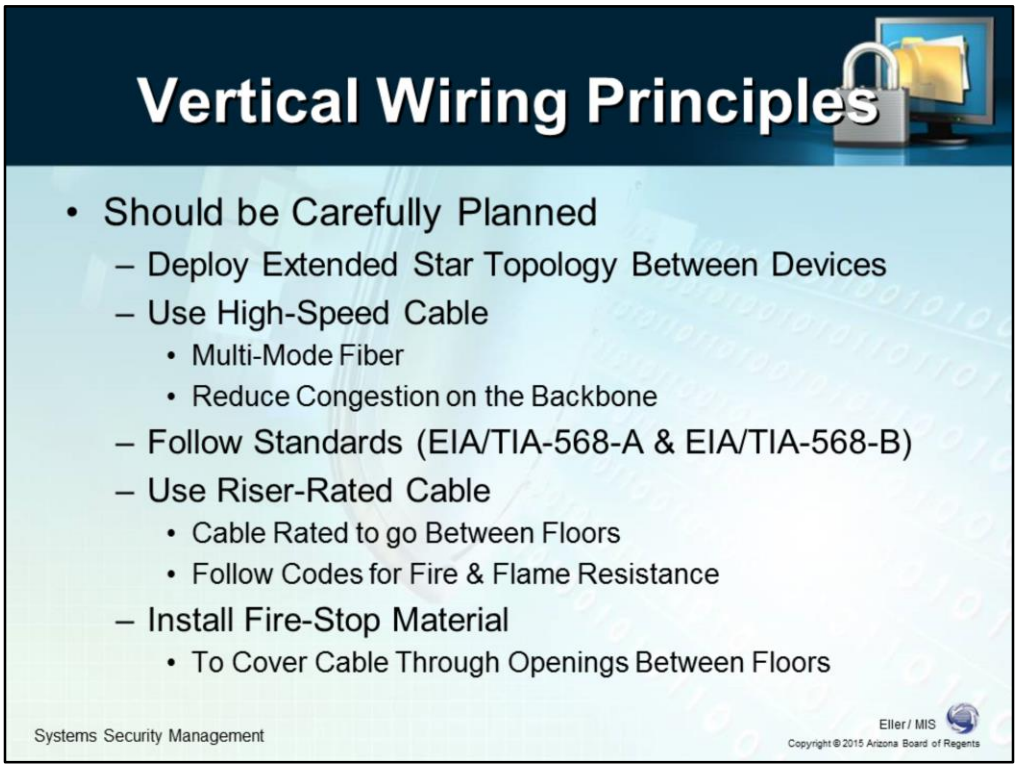
- Flexible Cabling
- Wiring Stations into a Physical Star
- Centralizing Cable Plant with Hubs/Switches
- Intelligence should be Built into Switches to Detect Problems
- Provide the Ability to Isolate Hosts & Servers
- The Ability to Provide High-Speed Links to Hosts/Servers



Implementing Structured Network Design

When designing a network structure in a building with multiple floors, many will typically deploy a horizontal star topology on each floor, connected by vertical wiring. Structured networks enables a SysAdmin to do the following:

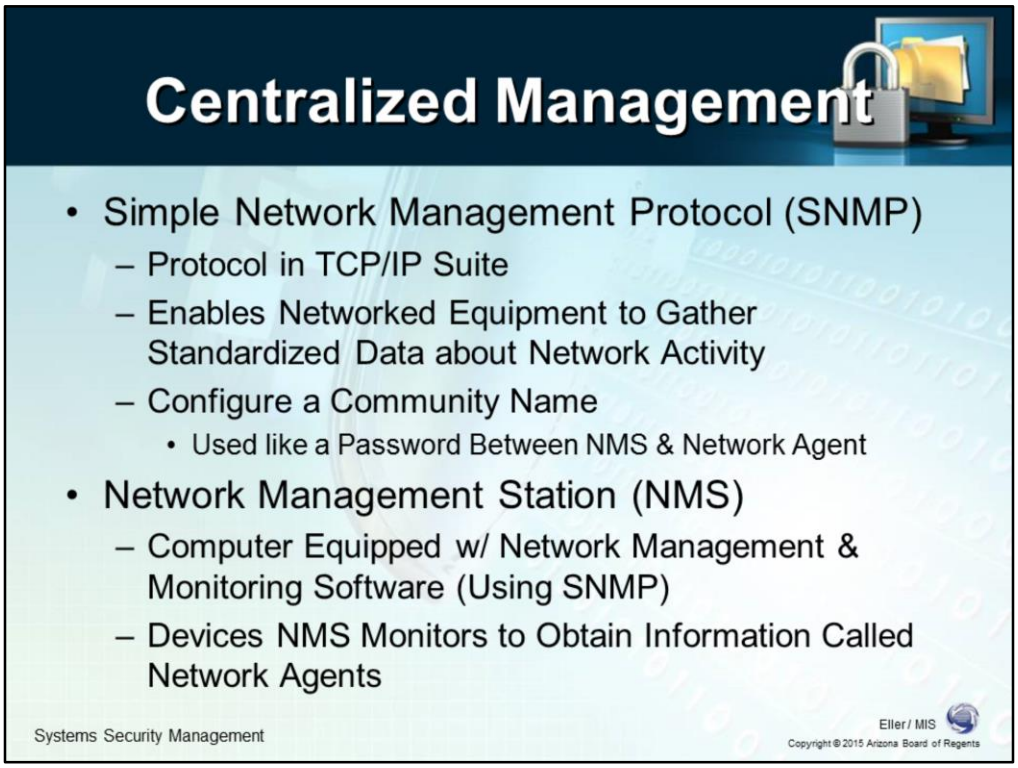
- Centralize or Decentralize Network Management
- Incorporate Vertical & Horizontal Design
    - Using High-Speed Communication on a Backbone
- Reconfigure Network Physically & Logically
    - For Security & Traffic Flow Management
- Segment Network According to Workgroup Patterns
- Add Redundancy
- Proactively Monitor & Diagnose Problems



Vertical Wiring Principles

Vertical wiring design should be carefully planned. Some considerations include:

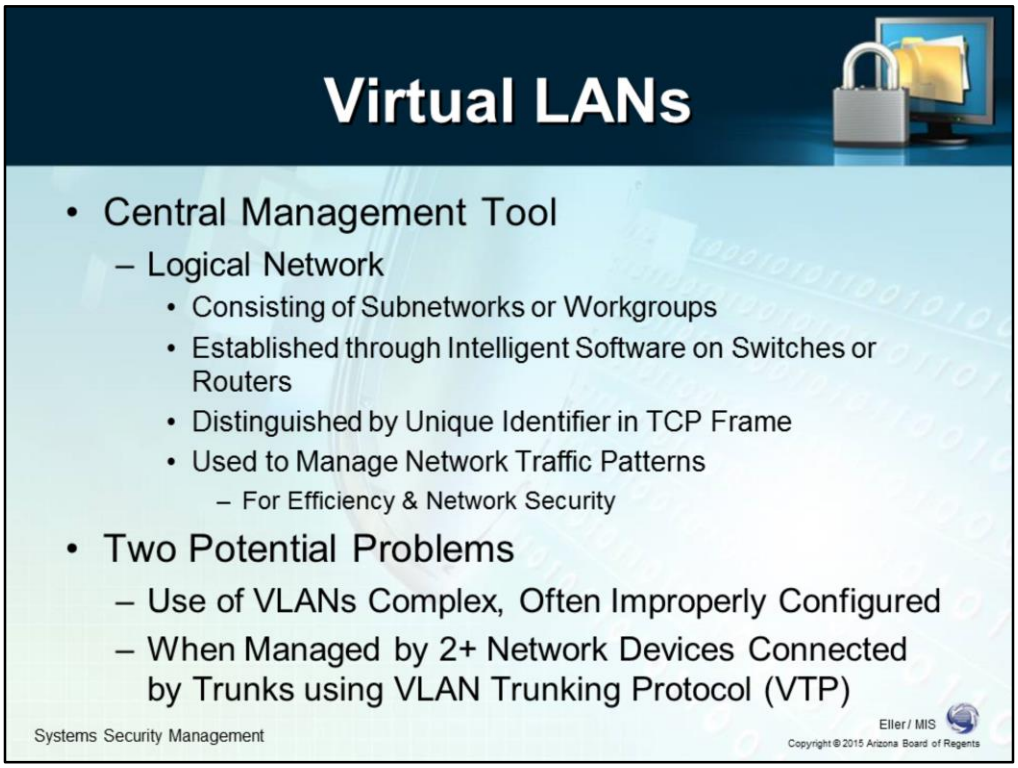
- Deploy Extended Star Topology Between Devices
- Use High-Speed Cable
  - Multi-Mode Fiber
  - Reduce Congestion on the Backbone
- Follow Standards (EIA/TIA-568-A & EIA/TIA-568-B)
- Use Riser-Rated Cable
  - Cable Rated to go Between Floors
  - Follow Codes for Fire & Flame Resistance
- Install Fire-Stop Material
  - To Cover Cable Through Openings Between Floors



Centralized Management

Centralized management of a network allows a SysAdmin to monitor and respond to network issues all from a single, centralized application or station. This is typically accomplished through the use of the Simple Network Management Protocol, or SNMP. This is a protocol in the TCP/IP suite that enables networked equipment, such as printers and switches, to gather standardized data about network activity. This is done by configuring a community name within the SNMP settings. This name is used like a password between a network management station and the network agents.

Network management stations are computers equipped with network management and monitoring software using SNMP. These devices monitor different network devices in order to obtain information. This information is referred to as a network agent.

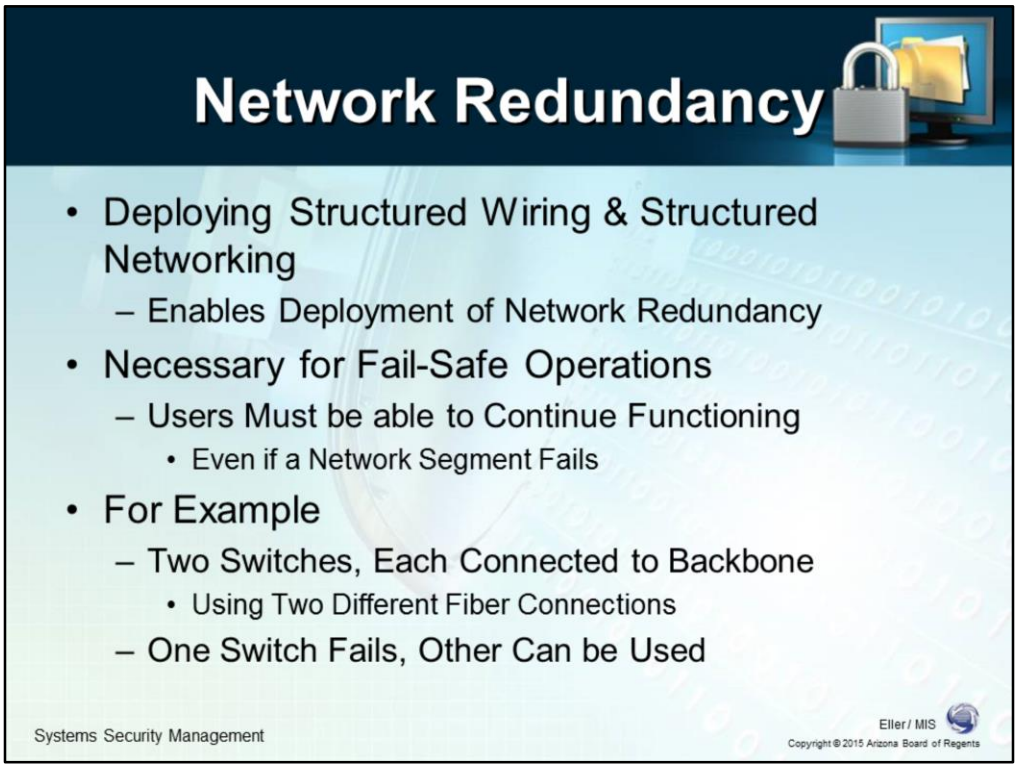


Virtual LANs

Virtual LANs are another type of centralized management tool commonly used on networks. VLANs are a logical network that consists of various subnetworks or workgroups. VLANs are established through the use of intelligent software that is configurable on switches and routers. VLANs are distinguished by a unique identifier in the TCP frame, and is typically used to manage network traffic patterns for efficiency and network security.

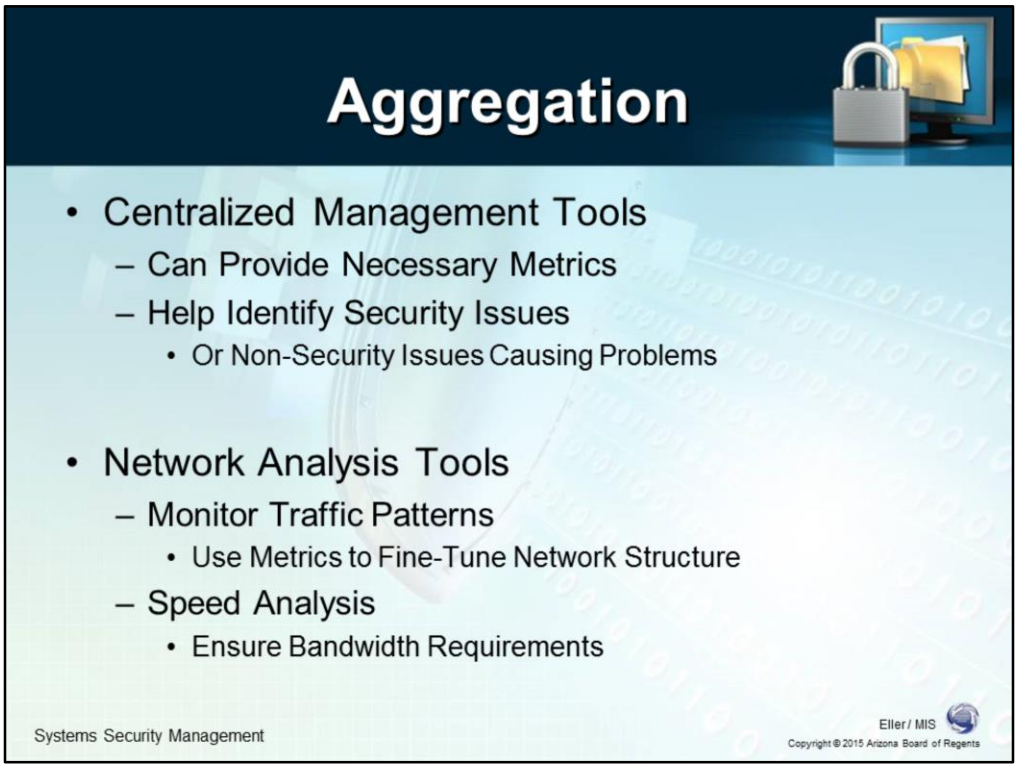
There are two potential problems with the use of VLANs. The first problem is that the use of VLANs is very complex, and because of this, they are oftentimes improperly configured. Another problem with VLANs is when they are managed by two or more network devices connected by trunks using the VLAN Trunking Protocol, or VTP.

The power of VLANs is shown when segmenting networks for security, despite physical location. For example, say Building A consists of mostly Finance staff and Building B houses HR. Normally just by physically separating a network segment, security can be attained. However, what happens if a move occurs and some of the staff from Finance move to Building B? Without VLANs, the network team would either have to reprogram the entire switch, or possibly even run new wiring to the computers in the new Finance area. By leveraging VLANs, the SysAdmin can easily separate the traffic on the switch with just a global config change, thus allowing HR traffic to go only to the HR PCs and Finance traffic to flow to the Finance PCs.



Network Redundancy

In order to create redundancy on the network, a SysAdmin will need to deploy structured wiring design along with structured networks. This enables an environment where network redundancy can be deployed. Redundancy is also necessary for fail-safe operations, where the users must be able to continue functioning even if a network segment fails. One way of enabling network redundancy would be to use two switches, each of which is connected to the network backbone using two different fiber optic cables. In this case, if one switch fails the other can be used in its place.



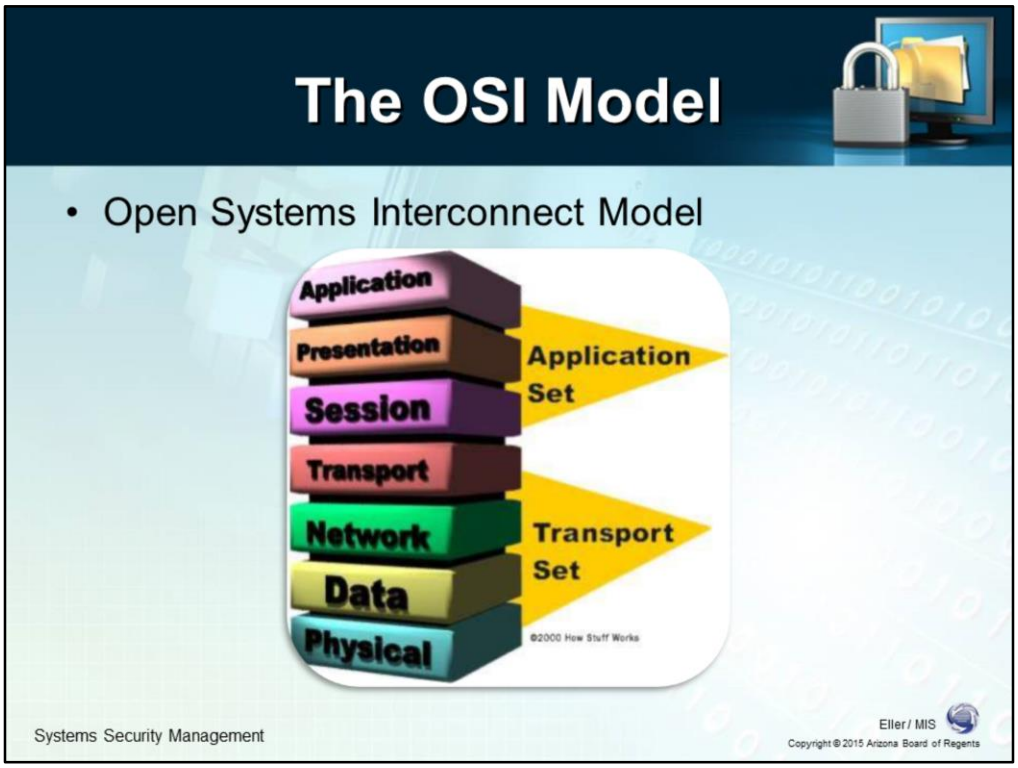
Aggregation

Centralized Management Tools

Depending on the centralized management tool a SysAdmin chooses to work with, the software can include features designed to provide the necessary metrics one can use to help identify security issues or other non-security issues that are causing problems on the network.

Network Analysis Tools

Network analysis tools are normally used to monitor network traffic patterns, the metrics they gather are then used to fine-tune the network structure. Speed analysis can also be used to ensure the network's bandwidth requirements are being met.



The OSI Model

Before the advent of the OSI reference model, communication with different entities and different vendors was extremely difficult. This was because every vendor would have a different mechanism to communicate. Therefore, to communicate with entities of different vendors, there arose a need to have a common platform. This need forced the International Organization for Standards to have a viable and universally accepted platform. Thus, the OSI reference model was born.

OSI Layers Explained

Physical Layer: The physical layer is at the bottom of this data networking model. It deals with crude data that is in the form of electrical signals. The data bits are sent as 0's and 1's. 0's correspond to low voltage signals and 1's correspond to high voltage signals. The mechanical aspects of communication, such as wires or connectors come under this layer. The physical layer also deals with how these wires, connectors, and voltage electrical signals work. Also, the process that is required for these physical aspects are taken into account in this layer itself.

The Data Link Layer: The transmission of the data over the communication medium is the responsibility of the data link layer. The 0's and 1's that are used in communication are grouped into logical encapsulation. This encapsulation is called frames. The responsibility for transporting these frames is that of the data link layer.

Network Layer: All over the world, there are many different types of ethernets. These networks are connected to each other through various media. When a data packet wants to reach a particular destination,

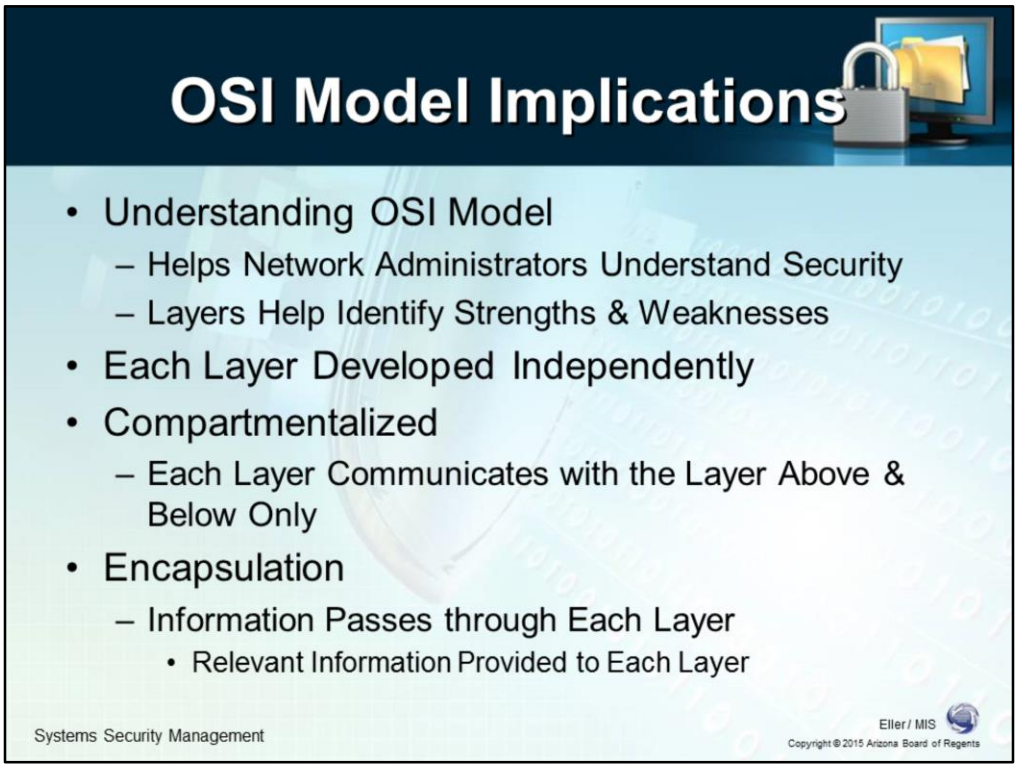
it has to traverse through these networks. Essentially, there are lot of operations that are taking place between the connected networks. Also, the packet data which is traversing, has to choose an optimum route, and the addressing of these packets has to be proper. The various operations between the networks, packet data issues, addressing and routing are handled by this network layer.

Transport Layer: The transport layer ensures quality and reliability of the communication. The data packet switching is entirely handled by the transport layer. There are basically two types of packet switching. They are connectionless packet switching and connection oriented packet switching. In connectionless packet switching, the packet data is allowed to choose the route in which it is going to reach the destination. Obviously, the packet in itself can't do this. Physical devices like routers are mainly responsible for the behavior of packets, but the packets formed from the same datum can reach their destination in different ways. Whereas, in connection oriented packet switching, once the route is decided, then all the packets have to follow the same route. Examples of connectionless packet switching are text messages in mobile phones, and the example of connection oriented switching is a direct voice call.

The Sessions Layer: The sessions layer is mainly responsible for creating, maintaining and destroying the communication link. PDU (Protocol Data Unit), in which various protocols are defined, that have to be followed during communication, are the responsibility of the sessions layer. The applications that use RPC's (remote procedure calls) are taken care of by the sessions layer.

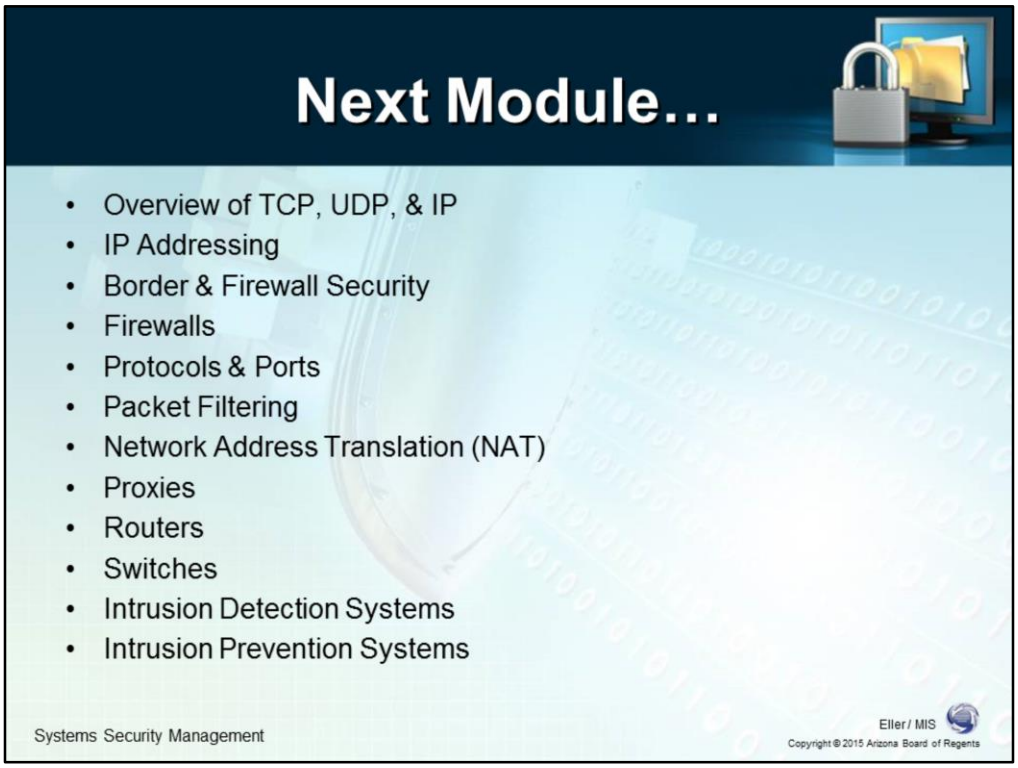
Presentation Layer: There are various techniques of data compression which are used to send and receive the optimized data. For example, if certain data is repeating itself for a number of times, then it is logical to send the data only once, and specify the number of times it is repeated. This bundling of the repeated data is one of the techniques of compressions. The compression and decompression of the data is handled by the presentation layer. Also, encryption and decryption techniques used to thwart malicious attacks on data are handled by the presentation layer.

Application Layer: This is the topmost layer of the OSI reference model. This layer comes into picture when there is a process to process communication. Whenever a user invokes any application, all the associated processes are run. Many a times, when an application wants to communicate with another application, then there has to be communication between these associated processes. The application layer is responsible for this interprocess communication (Lovekar, 2010).



OSI Model Implications

Understanding the OSI model helps network administrators understand the security of the network. Each of the layers help the SysAdmin to identify the strengths and weaknesses of their network. Each layer in the OSI model was developed independently, allowing for each layer to perform very specific functions. In addition, the OSI model is designed to be compartmentalized, allowing each layer to communicate only with the layer above or below it in the stack. This allows for data encapsulation, where information is passed through each layer; however, each layer will only receive the information that is relevant for continued communication.



In the next module we will be discussing Firewalls and Border Security, including:

- An Overview of TCP, UDP, & IP
- IP Addressing
- Border & Firewall Security
- Firewalls, Protocols & Ports
- Packet Filtering
- Network Address Translation (NAT)
- Proxies
- Routers & Switches
- Intrusion Detection & Prevention Systems

References

Carboy, R. (2010). Fire Suppression: How To Choose A Fire Suppression System For Your Server Room, Data Center Or NOC. *Ezine Articles*. Retrieved from http://ezinearticles.com/?Fire-Suppression-How-To-Choose-A-Fire-Suppression-System-For-Your-Server-Room,-Data-Center-Or-NOC&id=768738.

Lovekar, V. (2010). OSI Model Explained. *Buzzle.com*. Retrieved from http://www.buzzle.com/articles/osi-model-explained.html.

Overview of Computer Network Topology. (2007). *Networking Tutorials*. Retrieved from http://www.networktutorials.info/topology.html.

Palmer, M. (2004). Guide to Operating System Security, 1st Edition. *Thomson Course Technology*. Canada.

Rothke, B. (2008, October 3). The Lack of Security in a Fax Machine and How to Secure It. *Bright Hub*. Retrieved from http://www.brighthub.com/computing/enterprise-security/articles/8262.aspx.

Surman, G. (2002). Understanding Security Using the OSI Model. *SANS Institute*. Retrieved from http://www.sans.org/reading_room/whitepapers/protocols/understanding_security_using_the_osi_model_377?show=377.php&cat=protocols.