Network Infrastructure Design

Group Project

Lawrencia Agyemang | Will Glorius | Michael Agyei-Yeboah | IT 417 | 12/8/21

Contributions:
Michael - Title page, table of contents, mission statement & introduction to problem, created and designed network of strome college of business with description, security measures vii, viii, ix, x. Specifications Appliances & Software.
Lawrencia - Security measures taken i, ii, and iii.
William - Access Control, Firewalls, Intrusion Detection and Prevention Systems, Specifications

Table of Contents

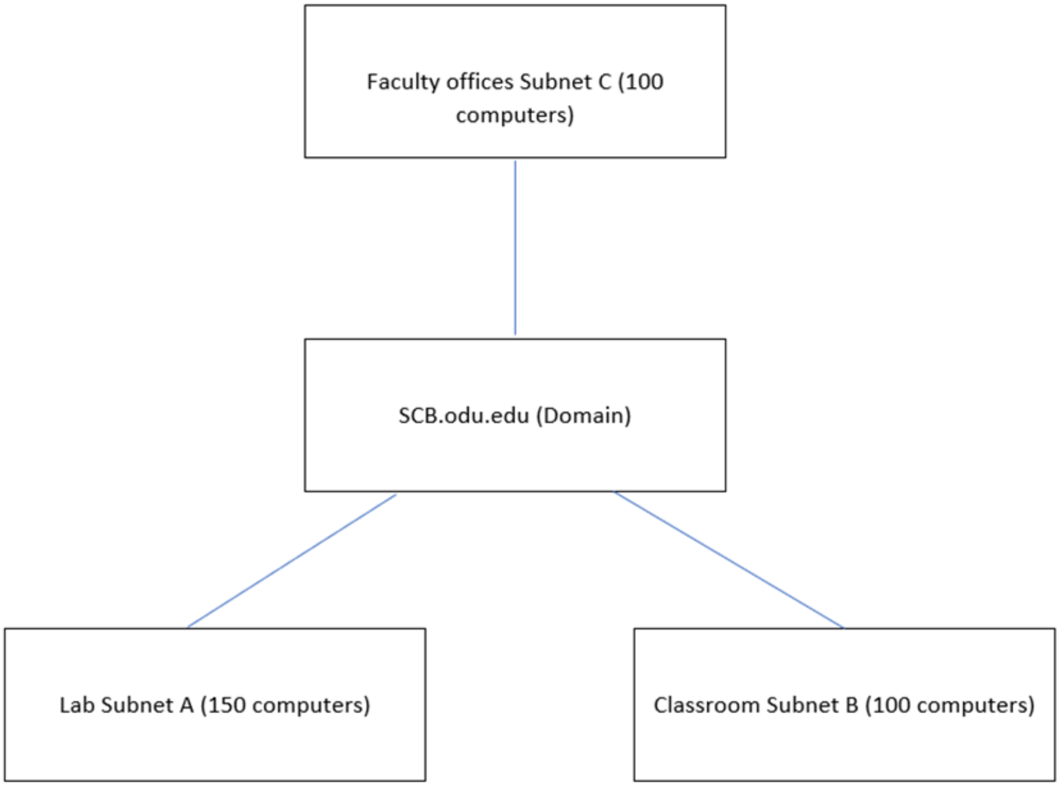
Introduction to Problem and Mission Statement

The problem is that the current topology for the Strome College of Business is inefficient. The current topology is outdated and requires optimizing for the increased network needs. Classrooms, faculty, and labs are receiving bad connections throughout the college of business. This requires updating switches, routers, and cabling. As classrooms and labs expand network usage and response times will increase. This is the current problem with the ODU network.

To combat this problem we are integrating more core switches and workgroup switches. The file server will help with faculty and students access the servers storage capacities. We also created multiple domain controllers. A domain controller authenticates and authorizes users in its network infrastructure. We created multiple domain controllers, because if one domain controller goes down the 2nd one will still allow users to authenticate themselves and access important information. ODU requires authentication to use any of its services any time you login. For faculty this is important as they cannot access services needed for teaching without authentication. Therefore, availability is crucial and should be online at all times.

Our mission is to ensure every student and faculty member has a reliable connection to the ODU domain to improve classroom instruction and deliver seamless . We will do this by integrating a star topology and rewiring cabling to each subnet to ensure a strong connection from the ODU domain. We aim to optimize better network usage, response time, and availability.

Network of Strome College of Business


Faculty offices Subnet C (100 computers)
SCB.odu.edu (Domain)
Lab Subnet A (150 computers)
Classroom Subnet B (100 computers)

We decided to use a star topology when designing this network infrastructure. The reasoning behind it is that there are only 3 subnets, and they must be wired so it is necessary they can all reach the domain. With the domain being in the middle it makes it much easier to access the network from anywhere in the college of business. Additionally, if need be, it is simpler to add more devices and connect them through each subnet without having to make any major changes with the design.

Wiring is tricky finding what is best suited for shorter or longer distances. So, it would be best to make an equipment room or telecom closet in the center of the building so that these devices can send signals to classrooms all over the building. A telecommunications closet is a small room that encloses telecommunications network systems and devices. Used for wiring devices connected in a local area network. An equipment room is a room or space within a building for the storage or installation of mechanical or electrical/electronic devices.

Regarding the cisco products the core switch is on the first floor alongside routers and the workgroup switches are on the second floor. We can assume that the network usage should be better due to quality core switches and servers. All in all, a faster network. Response times should increase due to the powerful core and workgroup switches and better cabling. Faculty and students will be able to enjoy noticeable faster speeds within the network. There should be no instances of where the network is down due to the strong connections between switches and cabling. Meaning a quality assurance of availability. This is also due to the choice of star topology. Meaning a quality assurance of availability.

Possible threats and attacks

Some of the possible threats and attacks to this network include;

- Viruses- These are computer codes that spread from computer to computer with the aim of stealing data or causing damage
- Adware- Unwanted software that monitors your online activities and bring you advertisements
- Malware- A code or file that spreads in a network stealing and virtually doing all the attacker wants
- Worms- A malware type that spreads in a network causing damage
- Phishing- Social engineering activity that tricks users to share sensitive information
- Spyware- Software that collects a user's information and shares with others causing social damage
- Denial of Service (DOS) attacks- Attacks that compromise a network making it inaccessible
- WI-FI attacks- Intrusion into a network and gathering the information shared therein
- Trojan horses- Legitimate-like codes that hide in the network or computer but cause damage.

All these possible threats can be addressed by using the following measures;

Use of strong passwords

System attacks are aided by the use of weak passwords. On the other hand, a system with strong passwords is less likely to get attacked, although not fully foolproof. It therefore means there is a significant chance of preventing attacks on your system if users use string passwords to access the system. This makes it hard for attackers. A strong password should contain a mixture of special characters, numbers, upper and lower case. All default passwords should also be cleared and reset to avoid the information being accessed by unauthorized people whether inside or outside of the organization. The IT department or person in charge should also train other employees on the importance of using strong passwords in their laptops.

Use of standardized software

Installing different software in the network system makes the system vulnerable to attacks, either by viruses, malware or spyware. To improve the network's security, installation of any software should have an approval. This can be done by ensuring that each employee's computer runs on the same plugins, extensions, browser, operating system or any other software the company uses.

Frequent monitoring of spam emails and taking proper action

One way security is compromised in a network is following prompts in an unknown email. Some employees may not be aware of such a danger and may innocently open such emails. To prevent this from happening, frequent monitoring is essential. Spam emails should be deleted immediately and such email addresses blocked. Employee training is also necessary to help them identify spam emails.

Use of firewall

A firewall is an integral part of network security. It involves setting a must-follow security path for all computers intending to access the network. Any computer that does not follow these rules is blocked. It helps protect the network from attacks because the intention of not following the access protocol may be mischievous. Thus, the threat is neutralized even before it happens.

Updating passwords

Changing passwords is one way of bolstering a network's security. Although the more the changes the better, too many changes may have its negative effects. These include users forgetting the passwords or the system having a self-defense system and treat the changes as threats; a change every three months is recommended and should follow the common practice of mixing characters.

Use of VPNs

The use of Virtual Private Networks (VPNs) boosts a network's security. It gives remote computers better and secure connection thus preventing unauthorized access into the system.

Training staff

To prevent data breaches staff must be trained. They need to know the impact of cyber-attacks. Some of the training areas include;

- Double and cross checking before sharing sensitive information
- Not clicking on any suspicious links
- Confirming email addresses before opening the attachments or links

Data backup

When attacks happen, data is the most targeted area. Although there are ways to retrieve data in crushed machines, backup is vital. It is therefore important to have a data backup policy to help have the data even under serious breaches. It also needs to be backed up frequently.

Planning, organization, risk analysis, and policies (Security planning)

Security planning, organization, and risk analysis are intertwined. Each leads to the next and if there is break or breach, then the rest fails. Planning involves the overall outlook of the network and what will be implemented. It also looks at the threats the network faces and how the security system will be arranged. This may involve the use of layered security where there are multiple access points each with a different set of measures. Alternatively, it may include a one stop point that is manned by an individual.

A security plan identifies and specifies what will be needed in the overall security. It also identifies all the services offered within the network. Each service may need a different security protocol from the other therefore a detailed analysis is crucial. The plan should be easy to follow to avoid complicating implementation which might bring the challenge of loophole creation. I will also detail everyone who has a role in the security implementation to avoid blame games and offer a clear path of reporting and responsibility.

The plan also considers other staff. It is crucial to have all users understand the plan and support it because the plan affects all

Organization

Security organization involves the resources necessary to implement the security plan. Generally, it is the length an organization will go to protect information from unauthorized access. This means it entails the procedures, people, and processes of protecting the information. More specifically, the people or staff will be trained on the processes and procedures.

Risk analysis

Risk analysis will involve identification and analysis of the possible threats. It involves a broad look such as natural calamities, and harmful/malicious human activity. The analysis comprises identifying the risk, what are the measures, and the frequency/probability of each risk occurring. The process of risk analysis involves;

- ➢ Taking a risk assessment survey from staff. It will involve creating a baseline of what are the possible risks that are likely to occur

- Risk identification. After having an idea of possible risks, this step entails the actual risks from the possibilities. It involves the possible damage to people, information and organization
- Risk analysis and their occurrence probability. This step involves identifying the frequencies of each risk occurring.
- Risk management development. It involves developing a plan of countering the effects of the risks once they occur or before they do.
- Risk management plan implementation. The plan developed will now start being implemented. The stage involves assigning responsibilities to specific individuals and identifying phases of intercepting the risks.
- Risk monitoring. Entails keeping an eye on the risks and how they happen.

Policies

It is a formal document detailing the rules, and processes to be followed in enforcement, management, monitoring, and maintenance of the network. Policies serve different groups and needs but they are categorized as general/ organizational, system-oriented, and issue-oriented. Organizational covers the entire organization, system, the network, while issue cover specific aspects such as user or use. The operationalization of the policies is done when any user needs access. They have to sign/accept them before proceeding to using the network.

The policy should at least cover key important areas especially on the threats and risks. These areas are change management, monitoring, use, backup, acceptable use, authentication, and authorization, among others.

Any measures you may take to ensure confidentiality and authenticity including encryption and VPNs

Confidentiality and authenticity are essential in data security. To determine these two the following questions should be answered;

- Can the information/data be released under specific conditions?
- Is the data valuable to unauthorized persons?
- Who are the authorized people or management level in the organization?
- Is the data sensitive and could it have an impact if released?

The measures to be taken include;

Encryption

This method of data confidentiality involves making information unreadable to unauthorized persons. It is only readable to people with a password and it helps to prevent the data falling to people who might use it maliciously. It is a necessary measure because if the data is used by unintended people or purpose it might cause damage to the organization or people it touches.

Manage and protect devices

Information stored in devices or networks need not be accessible to all. There can be restricted access depending on departments or seniority level. The application of suspending inactive sessions is crucial to promote confidentiality and authenticity. This is crucial in protecting some type of information. For example staff not needing access to financial documents can be restricted access to the information therein. Firewalls are also part of management and protection measures where devices that do not follow the set process are denied access. In terms of confidentiality, the use of a firewall can be used in tandem with passwords to restrict access to information to only authorized persons.

Safe Disposal

Whenever data is printed and no longer in use, safe disposal is crucial. This will prevent it from falling into wrong hands and used to damage the organization or people.

Data acquisition management

In collecting data, care should be taken to avoid collecting too much or collecting against the set rules

Access Control

Access control is a necessity; it dictates whether a user has permission to view, edit, or run: resources, documents, programs, and more.

Our most notable and first rule of access control is the principle of least privilege; a new user has basically no capabilities until placed into a group. When we create new users, we place them into the proper group: student, faculty, etc. These users then need to be authenticated; to ensure that a user is authenticated, they must use their password—something they know—followed by multi factor authentication using DUO Security to confirm they are who they say they are.

Furthermore, certain rooms on campus can't be accessed by just anyone; to ensure proper authorization, doors will remain locked until proper ID is placed on the sensor to allow the person access.

Firewalls

Firewalls are network security devices that monitor and filter incoming and outgoing network traffic. They can either permit or block data packets, depending on the set security rules.

The idea is to have a barrier between our internal network and incoming traffic from anyone or anything external that could be malicious—hackers or viruses. Our firewall will also regulate users already inside our network to prevent them from going to sites they should not and making any other prohibited connections. For our situation at hand, the most efficient, cost-effective firewall would be the renowned pfSense.

pfSense

pfSense is a free, popular, and open-source distribution of FreeBSD and is commonly used as both a firewall and router. In fact, it also features unified threat management, multi WAN, load balancing, and more. PfSense can be implemented using physical hardware or as software, and can be downloaded from its website www.pfsense.org. For our network, we will be using the Netgate 1541 BASE pfSenese + Security Gateway.

While pfSense may primarily be used as a router and firewall, there are numerous other purposes and features pfSense has to offer; in fact, pfSense even has a built-in package system which allows users to securely and efficiently expand their capabilities.

One of the nice benefits of choosing pfSense for our network is its fault tolerance: our network will remain up and running even when one or more parts of our network fail. We would remain connected to the internet through multi-WAN (channel bonding); multiple connections to the internet run simultaneously, allowing the connection to switch to the next connection if one were to fail. Furthermore, the division of connections may increase connection speed.

Similarly to our principle of least privilege in access control, our first and number one rule for our firewall policy is: deny by default; all inbound and outbound traffic is blocked until specifically permitted by the firewall rules. Not only does this decrease risk, but it also decreases the volume of network traffic. Configuring our rules to block and allow necessary traffic is simple; these settings can be found under the pfSense's "Firewall" tab and clicking on "rules". For example, pinging our network may be unnecessary, so we will ensure we block ICMP. Keep in mind, pfSense is a stateful firewall; this means it has memories of connections flowing through the firewall retained in the State Table.

Snort

Intrusion detection and prevention systems are essential for proper cybersecurity; these systems are not only designed to monitor and detect threats and vulnerabilities, but they can also block potential malicious activity. While there are different intrusion detection systems available, below we will discuss the installation and benefits of using the popular system "Snort."

Snort is a free, easy to use, open-source network intrusion detection and prevention system software available for both Linux and Windows. With its primary goals of detecting and blocking emerging threats, Snort provides real-time traffic analysis of networks and also functions as a packet logger. Snort is easy to install; in fact, it can easily be downloaded using pfSense's package manager.

Using a rule-based system, Snort combines protocol, anomaly, and signature inspection methods, with the goal of detecting and preventing malicious packets and activity such as: both denial of service and distributed denial of service attacks, buffer overflows, common gateway interface attacks, stealth port scans, and more. It is the rule language of Snort that determines the network traffic to collect and what should happen with malicious packets when detected; if malicious packets or activity is detected Snort will proceed to send alerts and notify the administrator that something is wrong. In fact, in some instances Snort will automatically take the first step and block the suspicious, potentially malicious activity.

Snort's ability to log packets is an essential capability; once we enable the packet logger mode, the proceeding packets will be collected and logged to the disk in a hierarchical directory. Once packets are collected Snort can perform an analysis of protocol; the data is captured in protocol layers. This assists administrators in examining transmission control protocol for malicious activity. In fact, Snort implements operating system fingerprinting; Snort can determine the platform of the operating system of a device or host that accesses our network. Furthermore, Snort enables administrators to debug both configuration issues and malicious packets.

Keep in mind, we must ensure that the rules are enabled and configured correctly in order for us to receive alerts of potential malicious activity; Snort alerts users based on the set criteria of what defines: malicious or unusual activity, vulnerabilities, and threats to network security and policy. We set this criteria by going to Snort's global settings, enabling the GPLv2 rule set, and updating our rules.

Host Hardening Update Policies and Implementation

Hardening strategies usually consist of locking configurations to achieve a balance of operational functionality and security. Another important part of this effort is vulnerability management and change management. It adds visibility and controls to help you stick to a strict build standard. All possible faults that threat actors might exploit to hack into a technical equipment, system, or network are referred to as the "attack surface." The goal of system hardening methods and approaches is to limit the attack surface and mitigate as many vulnerabilities as feasible.

While system hardening demands a significant and ongoing effort, it garners significant benefits for businesses. Here are a few noteworthy advantages: Increased security - the goal of system hardening approaches and technologies is to limit the attack surface. As a result, the danger of malware, unauthorized access, data breaches, and other unwanted behavior is considerably reduced. Improved system performance - is the most common system hardening best practices it is used to reduce the number of applications and activities. This leads to fewer system failures, a lower risk of software bugs affecting user functions, fewer inconsistencies, and a lower risk of cyber threats, all of which impede user performance. System hardening approaches may help change a complicated system into a simpler one with less applications and services, as well as a more stable and reliable setup. This results in a much more visible and plain environment that is easier to manage and audit. By automating updates and patches, you can keep an operating system in a hardened condition. While operating systems are also software, operating system hardening differs from conventional application hardening in that the software in this case is in charge of issuing rights to other programs.

Operating system hardening methods include: Installing the most recent updates from the operating system's developer (i.e. Microsoft, Apple). Using third-party EPP/EDR software or enabling built-in security capabilities such as Microsoft Defender. Drivers that are no longer in use are being deleted, and those that are still in use are being updated. Limiting the number of peripherals that can be attached Encrypting the host disk with a hardware TPM. Activating Secure Boot. Putting a cap on system access rights. On top of passwords, using biometrics or Fast ID Online (FIDO) authentication.

Establishing a strong password policy, securing critical data with Advanced Encryption Standard (AES) encryption or self-encrypting drives, installing firmware resilience technologies, and multi-factor authentication are all other techniques for hardening server systems.

When used in conjunction with an instruction prevention and detection system, these system hardening techniques can significantly limit the attack surface of the network: Network firewalls must be configured correctly. Network rules and access rights audits. Disabling network ports and protocols that are no longer in use. Disabling network services and devices that are no longer in use. Encryption of network traffic.

Establishing a baseline is a necessary first step in hardening a system. The baseline is a hardened state of the system that you should strive for and then monitor for any deviations from that hardened state.The first step we did was using a benchmark to perform an assessment of the targeted hardened system, to understand how well the current configuration matches the relevant benchmark. This initial assessment lets us identify areas where the system is not aligned with the required hardening baseline. Based on the assessment, we modified system configuration to meet security recommendations. Hardening a system to meet benchmark standards is only the first step. We continued to conduct periodic follow-up assessments to ensure that the system is still aligned with the hardening baseline. Any configuration or file changes could make it vulnerable to attack. In order to maintain a hardened state, we constantly re-evaluate and remediate any change to the system that violates the security benchmark.

Security for software/applications policies, configurations, and what/who may install software

Only administrators and authorized personnel will be granted permission to install software. We configured the system restricting users without admin fewer control and permissions. It helps with identifying who can access the network and authorized use of resources. These security policies will help secure domain controllers, servers, client devices, and other private information. Some of these policies are account, local, application control, and windows firewall. These deal with password security, account security, and restricted/unrestricted access in system services. Generally changes to these policies will not be immediate and take a quick refresh. To keep software secure it is required to keep it up to date and to download it directly from the company. Protecting networks safe from vulnerabilities and potential exploits.

Data protection policies, technology, backup storage locations, and restoration/recovery measures.

A data protection policy (DPP) is a type of security strategy that aims to standardize data use, monitoring, and administration. The major purpose of this policy is to preserve and secure any data that the business consumes, manages, and stores.All data kept by the organization's core infrastructure, including on-premise storage devices, offsite locations, and cloud services, should be covered by data protection rules. It should assist the company in ensuring the security and integrity of all data, both at rest and in transit.

Data protection policies can reflect a company's commitment to maintaining consumer data security and privacy. If the company is subjected to compliance audits or suffers a data breach, the data protection policy can be used to illustrate the company's adherence to data security standards.

Our data protection policy consists of the following aspects:

- The extent to which data protection is needed
- Individuals, departments, devices, and IT environments all use various data protection strategies and regulations.
- Any data protection law or regulatory obligations that apply
- Data custodians and jobs expressly accountable for data protection activities are among the roles and duties connected to data protection.

Steps to developing a data protection policy

1. Introduction and scope—the data protection policy should begin with a description of what it is for and how to utilize it. Employees will understand the relevance of the document and why they should acquaint themselves with its concepts as a result of this. This section should also define the DPP's scope, including the types of data it covers and the people who are responsible for it.

2. Definitions—to avoid any misconceptions among your organization's members, this section describes the different terminology used in the paper.
3. Principles of the General Data Protection Regulation (GDPR)—explains the requirements of the General Data Protection Regulation (GDPR) (GDPR). This is necessary to ensure that employees understand their responsibilities and adhere to data protection guidelines.
4. Data processing that is lawful—the GDPR states that data processing is legal if it is based on six legal grounds. The data must be treated differently depending on the legal categorization.
5. Employees are allocated distinct data protection tasks and obligations, and it is critical that each employee knows his or her responsibilities. If your business has many teams or employees that handle personal data, it's critical to lay out the authority structure for data security.
6. Procedures for data breach notification—notification is an important part of a DPP. In the case of a data breach, everyone in your company has to know what to do. Your response to a data breach might be scrutinized by the courts.
7. Data subjects' rights—this is a list of consumer rights that reminds employees of their responsibilities. Consumer data can only be kept for as long as it is required to offer a service.
8. Your DPP should include information on your organization's security measures, data retention processes, and data records.
9. Contact information—employees should know who to contact if they have any issues or questions regarding data security (perhaps a Data Protection Officer). Make sure you include all necessary contact information.

A disk or tape backup that replicates specific information to a disk-based backup system so it may be safely kept is one storage technology that businesses can utilize to protect data. Tape-based backup is a great way to secure your data from cyber-attacks. Although tapes are difficult to access, they are portable and intrinsically offline when not put onto a drive, making them safe from network attacks. In disk-based backup, data deduplication, also known as data dedupe, is important. Dedupe reduces the amount of storage space required for backups by eliminating redundant copies of data. Deduplication can be a software-enabled feature in disk storage or it can be included into backup software. Dedupe software uses pointers to find unique data copies to replace superfluous data blocks. Only data blocks that have changed since the last backup are included in subsequent backups. Deduplication originated as a data-protection technique, but it has now evolved into a critical feature for reducing the amount of capacity required for more costly flash storage. Mirroring allows businesses to produce an exact clone of a website or files that can be accessed from many locations.

Continuous data protection (CDP) backs up all of an enterprise's data anytime a change is made, whereas storage snapshots can automatically construct a collection of pointers to information saved on tape or disk, allowing for speedier data recovery. CDP has become a critical component of disaster recovery, allowing for quick recoveries of backup data. CDP allows businesses to roll back to the most recent good copy of a file or database, lowering the amount of data lost in the event of data corruption or loss. CDP began as an unique product category, but it has since developed into a feature of most replication and backup programs. Additionally, CDP can remove the requirement for numerous copies of data. Organizations instead keep a single copy that is constantly updated as changes occur.

Incident Response Plans & Disaster Recovery Plans

Disaster recovery plans and incident response plans are similar yet distinctive. An incident response plan is the systematic and layered approach to how your organization will respond to cyber incidents, whether that be hackers, infections, or just general failures. The main distinction is in their major goals. An incident response plan's goal is to secure sensitive data in the event of a security breach, whereas a disaster recovery plan's goal is to keep business operations running after a service disruption. Disaster recovery plans can be broken down into three main topics: what to recover, who and how's being recovered, and what your recovery objectives are. Incident response plans have three main components:Who is involved, what are our objectives, and how are they going to be accomplished.

A Disaster Recovery Strategy (DRP) is a business plan that explains how to continue operations promptly and efficiently following a disaster. Disaster recovery planning is a subset of business continuity planning that addresses aspects of a company's operations that rely on IT infrastructure.The overarching goal is to devise a strategy that will enable an IT department to recover enough data and system functionality to allow a business or organization to function - even if just to a bare minimum. The process of creating a DRP starts with a proposal to get upper-level management support. Then a business impact analysis (BIA) is required to establish which business operations are the most vital, as well as the needs for restoring those functions' IT components following a disaster, whether on-site or off-site.

Scope and Objectives of a Disaster Recovery Plan

The Disaster Recovery Plan establishes a preparedness that allows for rapid staff reaction in the event of a disaster. As a result, the recovery effort will be more effective and efficient.

The Disaster Recovery Plan should be created with the following goals in mind:

1. Minimize the duration of an important application service outage to reduce the extent of any loss.
2. Examine the damage, fix the damage, and turn on the computer center that has been repaired.
3. Recover data and information necessary to core application operation.
4. Maintain a well-organized and efficient recovery operation.

5. Train technology staff to respond quickly in the event of a crisis.

Every company is responsible for responding to any service disruption, whether it is temporary or long-term. Businesses will be able to restore key application availability in a timely and structured manner following a disaster if they establish, document, implement, and test this Disaster Recovery Plan. Senior management, end users, and staff departments will all be needed to help the technology department achieve these goals. A crisis or catastrophe warning procedure triggers Disaster Recovery Plan operations. Technology management will be notified of a potential disaster at the computer center if an event is discovered. The Recovery Management Team will assess the situation and decide whether or not a disaster should be declared and the Disaster Recovery Plan implemented. The chosen recovery staff will be alerted and directed to commence their recovery activities as soon as the Plan is implemented.

Types of Disaster Recovery Plan

There is no such thing as a perfect disaster recovery plan that is ready for any attack. However, to ensure our disaster recovery covered every aspect we incorporated preventive measures, detective measures, and corrective measures. Preventative actions will be taken to try to avoid a disaster. These procedures are aimed at identifying and mitigating hazards. They are intended to lessen or avoid the occurrence of a specific event. Data should be backed up and stored offsite, surge protectors should be used, generators should be installed, and periodic checks should be performed. To identify the presence of any harmful activity inside the IT infrastructure, detective steps are used. Their goal is to find new threats that may exist. They may be able to detect or expose unwelcome events. Installing fire alarms, utilizing up-to-date antivirus software, providing employee training sessions, and installing server and network monitoring software are all examples of these procedures. Corrective actions are intended to restore a system after a disaster or other unwelcome event. These actions are aimed at repairing or restoring systems following a calamity. Following a "lessons learned" brainstorming session, corrective steps might include maintaining vital papers in the Disaster Recovery Plan or getting suitable insurance coverage. At least three fundamental questions must be answered in a disaster recovery plan: what is its goal and purpose, what team members will be in control in the event of a crisis, and how will these people do when it comes to following the procedures when disaster occurs.

Stages of a Disaster Recovery Plan

A DRP's purpose is to restore normal computing services in the shortest amount of time achievable. There are multiple steps in a typical DRP, including the following:

- Understanding the operations of an organization and how all of its resources are linked.
- Assessing the susceptibility of an organization in all aspects, including operational processes, physical space and equipment, data integrity, and contingency preparation.
- Understanding how a calamity will influence the company at all levels.

- Creating a short-term recovery strategy.
- Creating a long-term recovery strategy, which includes determining how to restart regular business operations and prioritizing the functions that will be resumed in that order.
- As the business changes, the strategy must be tested and updated on a regular basis.

Phases in Developing an Effective Disaster Recovery Plan (DRP)

- Business Impact Analysis (BIA): Developing an effective Disaster Recovery Plan requires doing a thorough and extensive Business Impact Analysis (BIA). During this phase, the system's needs, functionalities, and interdependencies are examined, with the results being utilized to identify system contingencies and prioritize tasks. The Disaster Recovery Plan is driven by the Business Impact Analysis, which identifies the applications and systems that will have a substantial impact on the business in the case of a disaster. Obtaining feedback from departments across the company, from Human Resources and Customer Service to Information Technology and Accounting, is critical during this phase. The BIA is a useful technique for educating the company about the importance of a Disaster Recovery Plan and identifying any alternative manual operations that might potentially lessen the impact of a system outage, in addition to using this knowledge to keep system availability.
- BIA is dependent on identifying the Recovery Point Objective (RPO) and the Recovery Time Objective (RTO) (RTO). The RTO is the entire amount of time an IT component may be in recovery before negatively impacting important business activities; the RPO is the point in time to which data must be restored. Because various applications and IT components have varied RPOs and RTOs, the analysis is critical. An application that serves a mission-critical application, such as client order processing, may have a quick RPO/RTO, but an internal, non-customer facing program with minimal import may have a much longer RPO/RTO.
- Creating a Plan for Your Recoveries A thorough approach is required when developing a good Disaster Recovery strategy. Network requirements, infrastructure requirements, data recovery, data and record management, security, and compliance are all important factors to consider. Following the identification of essential applications and data recovery objectives, the organization must develop particular methods and solutions to ensure that the recovery targets for apps, networks, and data are met within the specified timeframes. Meeting these recovery goals may necessitate the internal deployment of new architecture, tools, and infrastructure, or the use of an external service provider. Electronic vaulting, tape retention, and a twin data center strategy are all options to explore.
- Testing and Educating: A great Disaster Recovery Plan requires careful research and the development of sound recovery procedures; nevertheless, testing the plan and training employees on how to execute it is crucial to effective DR planning. The only

way to assure that your plan will work is to test it frequently and provide a mechanism to ensure that it is updated to reflect changes in the environment. There are various levels of testing, with varying degrees of involvement, ranging from a structured walk through with key technical resources verbally assessing the plan, to simulation testing, in which a disaster is simulated so that the plan can be implemented, to full interruption testing, in which the disaster recovery plan is fully activated. The company must develop the necessary tests in order to adequately analyze the plan's validity. Along with testing the plan, allocated people must be trained on their responsibilities in the disaster recovery scenario as well as the plan's overall content. The company, like testing, must reassess the training strategy on a regular basis to handle the inevitable organizational changes, new employees, and attrition.

Key Elements of a Disaster Recovery Plan (DRP)

Only part of a disaster recovery plan is ensuring that your assets, data, and hardware are safeguarded; the rest is creating a method for getting back up and running as rapidly as possible. It's time to make a strategy rather than trying to put the pieces back together after a huge storm. The seven essential aspects of a corporate disaster recovery strategy are listed below.

- Communication Plan and Role Assignments: Communication is critical in the event of a disaster. A strategy is necessary because it brings all employees on the same page and ensures that every communication is properly defined. Employee contact information should be updated in documents, and staff should know exactly what their duty is in the days after the incident. If you don't have a technical resource to assist you go through everything, you'll need assignments for jobs like setting up workstations, analyzing damage, diverting phones, and other chores.
- Protect Your Equipment: When a large storm is approaching, it's critical that you have a strategy in place to safeguard your equipment. You'll need to get all of your equipment off the floor, into a room with no windows, and securely wrapped in plastic to prevent water from getting to it. It's certainly desirable to totally seal equipment to keep it safe from flooding, but this isn't always possible in catastrophic floods.
- Data Continuity System: When putting together your disaster recovery strategy, think about what your company needs to function. You must know exactly what your business requires in terms of operations, finances, supply, and communications. Whether you're a large consumer company that needs to fulfill shipments and communicate with customers about those shipments, or a small business to business company with multiple employees, you should document your requirements so that you can make backup and business continuity plans and have a complete understanding of the requirements and logistics.

- Make sure your backup is up to date, and include a comprehensive local backup of all servers and data in your disaster recovery strategy. Run them as far ahead of time as necessary, and make sure they're backed up to a safe location that won't be affected by the calamity. It's also a good idea to save that backup on an external hard disk that you can take with you offshore in case something goes wrong.
- Workstations, their components, servers, printers, scanners, phones, tablets, and other technology that you and your workers utilize on a regular basis should all be included in your detailed asset inventory plan. This will serve as a quick reference for insurance claims following a large tragedy, as it will provide your adjuster with a short list (with photographs) of any inventory you may have.
- Pictures of the Office and Equipment (Before and After Preparation): In addition to the photos of individual inventory items that you should have, you'll want to take photos of the office and your equipment to show that those items were in active use by your employees and that you took the necessary precautions to move your equipment out of harm's way in preparation for the storm.
- Vendor Communication and Service Restoration Plan: As soon as the storm passes, you'll want to be back up and running. Make sure to incorporate vendor communication in your strategy. Check with your local power company to see if there will be any power spikes or outages while the damage is being fixed. Checking with your phone and internet providers about repair and access is also a good idea.

Testing Criteria and Procedures for Disaster Recovery Plans

DR strategies should be extensively tested and assessed on a regular basis, according to best standards (at least annually). Documentation and processes for testing the strategy are included in comprehensive DR plans. The tests will offer confidence to the company that all relevant processes have been included in the strategy. Testing is also done for the following reasons:

- Choosing backup facilities and processes that are both possible and compatible.
- Identifying aspects of the strategy that require change.
- Providing team supervisors and members with training.
- Demonstrating the organization's capacity to recover.
- Providing motivation to maintain and update the disaster recovery strategy.

Reviewing a Disaster Recovery Plan

There are three common ways to review a plan:

- The system that is being evaluated. An organization may put the system to the test. Processes for recovery and backup are constantly put to the test. For example, turn off the power to a system to watch how quickly the firm recovers.

- A tabletop exercise is now in progress. These are scenario-based exercises in which a facilitator presents a scenario and asks exercise participants questions about the situation, eliciting a discussion among the participants regarding roles, responsibilities, coordination, and decision-making. A tabletop exercise involves only talking and does not need the deployment of equipment or other resources.
- A functional exercise is now being performed. Workers can fulfill their roles and responsibilities in a controlled setting, just as they would in a real-life emergency. The purpose is to put particular members of the team, procedures, and assets engaged in one or more recovery plan components to the test.

Incident Response Plan

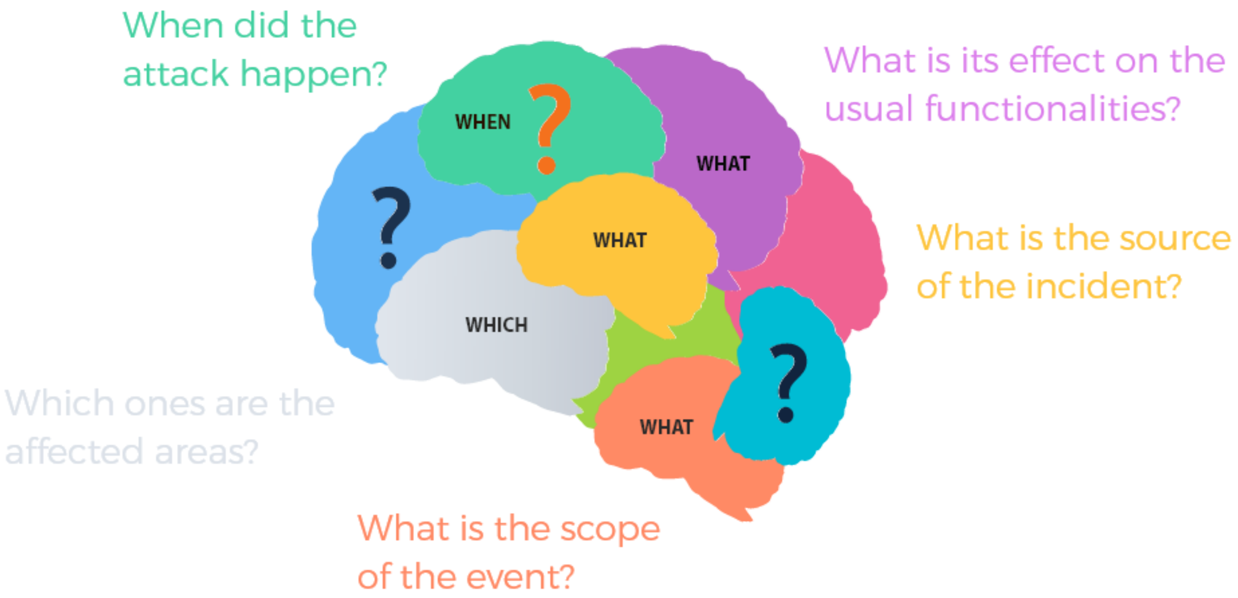
Phase I – Preparation

The IR team's initial response to any attack requires extensive planning. This phase is all about putting in place suitable processes and instruments before an issue occurs. The following are the important steps in this phase: Identifying the most critical assets and putting in all of your efforts to defend them, and data from previous instances was analyzed. It would be useful to have a few significant tools and resources in your arsenal to deal with events. You must have a diverse arsenal of weapons. Your organization should, for example, have a backup plan in place if one of your communication and coordination platforms fails.

Begin creating security policies for the domains that are necessary. These areas can include everything from basic information security to network security, server security, application security, and more. Create a method for dealing with events once you've specified all of your policy criteria. Prioritize issues, identify roles and duties, remediate events, and provide tools for handling various incident responses, incident paperwork, and both internal and external communications while planning.

Phase II – Identification

The identification of the actual occurrence is the first step in the second phase. Start by answering the following question: Is this uncommon behavior? Examine the impacted sections of the network or system once you've determined the sort of occurrence. Suspicious activity, unexpected new files, strange login attempts, unexpected user logins or user accounts, and so on will be on your radar. Examine the problem thoroughly since it will make the next steps easier. You can analyze the issue by asking yourself a few simple questions:


When did the attack happen?
What is its effect on the usual functionalities?
What is the source of the incident?
Which ones are the affected areas?
What is the scope of the event?
WHEN
WHAT
WHAT
WHICH
WHAT

It's time to examine the sort of occurrence you're dealing with once you've assessed the scenario. An event is usually divided into six categories: Unauthorized entry, services being denied, code that is malicious, inappropriate use, scans, probes, and attempts at access, incident under investigation. The procedure is made easier by incident identification. Incident detection using several methods with various levels of information. This might be detected either automatically or manually. Network- and host-based IDPs, antivirus software, and log analyzers are examples of automated detection capabilities. However, in the event of manual detection (which is frequently mentioned by users as an issue), it can be identified or not. A large number of possible incident symptoms. On a daily basis, a large-scale business, for example, gets hundreds, if not millions, of intrusion detection sensor alerts. For the precise and effective analysis of incident-related data, specialist technical skills and substantial experience are required.

An incident's signals might be classified as either antecedents or indicators. Precursor signals suggest that an incident may happen in the future, whereas indicators indicate that an occurrence has happened or is happening now. IDPS, antivirus, anti spam software, file integrity checking software, third-party monitoring devices, operating system and service/application logs, network device logs, information on new vulnerabilities and exploits, and people from within and outside the organization are all common sources of precursors and indicators.

Phase III – Containment

After gathering all required information on the incident, the IR team should now focus on containing the danger in order to prevent future harm. The initial step in this phase should be to disconnect the infected machine from the network and back up all of the infected system's sensitive data. After then, you might choose for a temporary remedy to guarantee that the harm caused by the occurrence does not worsen. The major purpose of this phase is to keep the incident's scope and size as little as possible. Make sure you know how well your infected machine or network is working. You can choose from the following choices to decide this: Option 1: Disconnect the infected object and allow it to continue operating independently. Option 2: Immediately shut down the entire system. Option 3: Allow the machine to function normally while continuing to watch its operations. All of these options are viable options for dealing with the problem at hand.

Following the implementation of a successful containment strategy, it's time to focus on evidence collecting and management, which isn't something that happens very often. Most malware events, for example, do not qualify for evidence collection and processing in many businesses. The advantages of obtaining evidence are not restricted to settling an occurrence; it also aids in legal processes. Keep a detailed record that details the methods for preserving all traces of evidence, including infected systems. Evidence should always be accounted for when it is transferred from one party to another. The evidence log should include the following information: Serial number, model number, hostname, MAC and IP addresses, and location are all examples of evidence identifying information. Name, title, and phone number of the evidence holder. For each instance of evidence processing, record the location, time, and date, as well as the time zone.

Phase IV – Eradication

The IR team should be working on a lasting solution in this fourth phase, which should include a mechanism for restoring all affected organizations. Eradication is a straightforward procedure for removing a danger from an infected network or system. This phase should begin only after all other internal and external tasks have been accomplished. The following are the two most significant components of this phase: Clean-up: Running a powerful antimalware and antivirus program, uninstalling the infected software, restarting or replacing the entire operating system and hardware (depending on the magnitude of the event), and rebuilding the network are all steps in the clean-up procedure. Notification: In accordance with the reporting chain, notify all staff affected. It is recommended that various common event "playbooks" be created to assist the IR team in maintaining a consistent approach to the issue.

Phase V – Recovery

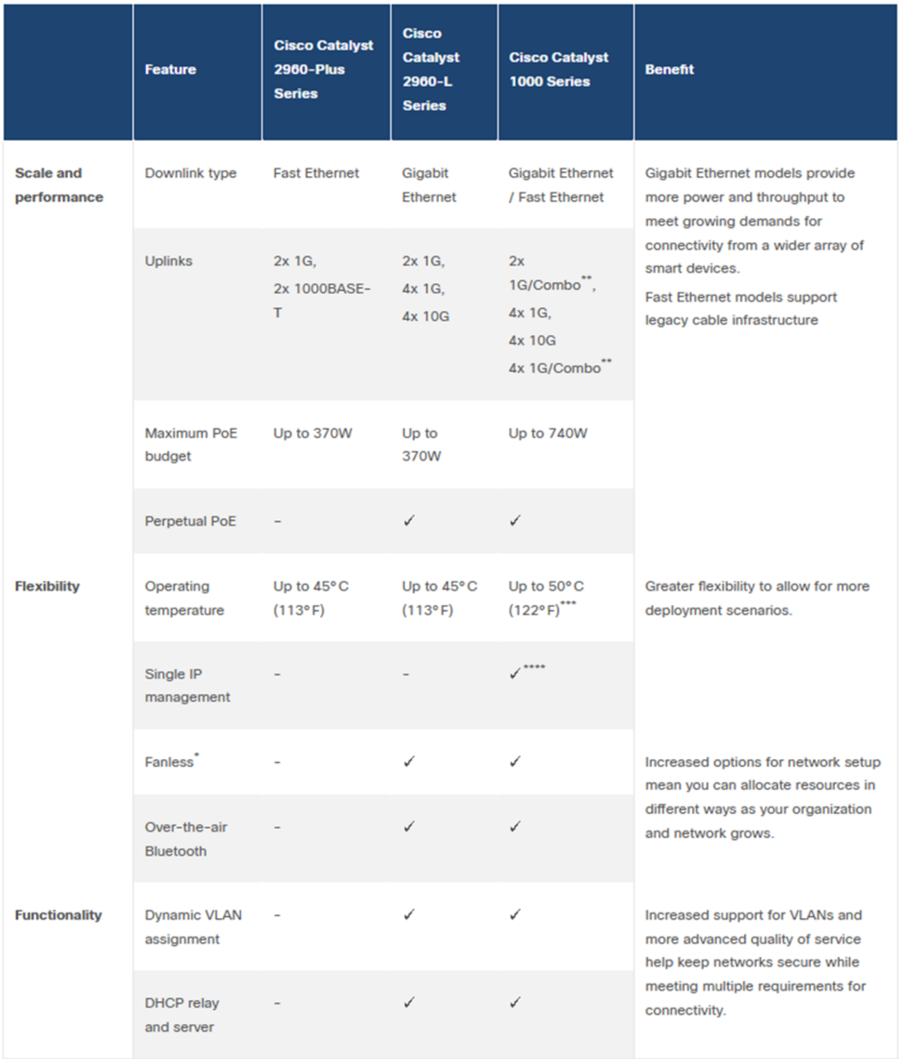
The compromised system or network will be brought back to life at this point. This phase includes everything from data recovery to any remaining restoration procedures. It happens in two stages: Service restoration will be carried out in accordance with the company's contingency preparations. System/network validation entails putting the system/network through its paces and ensuring that it is in good working order. This phase ensures that the infected entity is both secure and functional once again.

Phase VI – Lessons Learned

Maintain a full record of the whole occurrence when the investigation is completed. This final step will maintain your organization ready for any future attacks while also allowing you to extract value from them. Following the effective management of an event, the IR team should convene a review meeting. Pay special attention to the identification of essential changes for existing security controls and processes at this "lessons learned" discussion. Periodic meetings like this can genuinely help to reduce incidences. Ascertain that this review meeting aids you in discovering current security flaws and policy and procedure issues. You have the option to revise your existing IR strategy based on the outcomes of this discussion. Your IR team will change as a result of this step to reflect new risks and enhanced technologies. This comprehensive paper may also be used to teach new team members. After each occurrence, produce a follow-up report for future use as the final step of this phase. Another recommended practice for the IR team is to send out an awareness message to senior management as well as all employees about what transpired (in the event of an incident) and what lessons the IR team learnt. If the incident has an impact on the end-user, the message might include them.

Specifications Appliances & Software

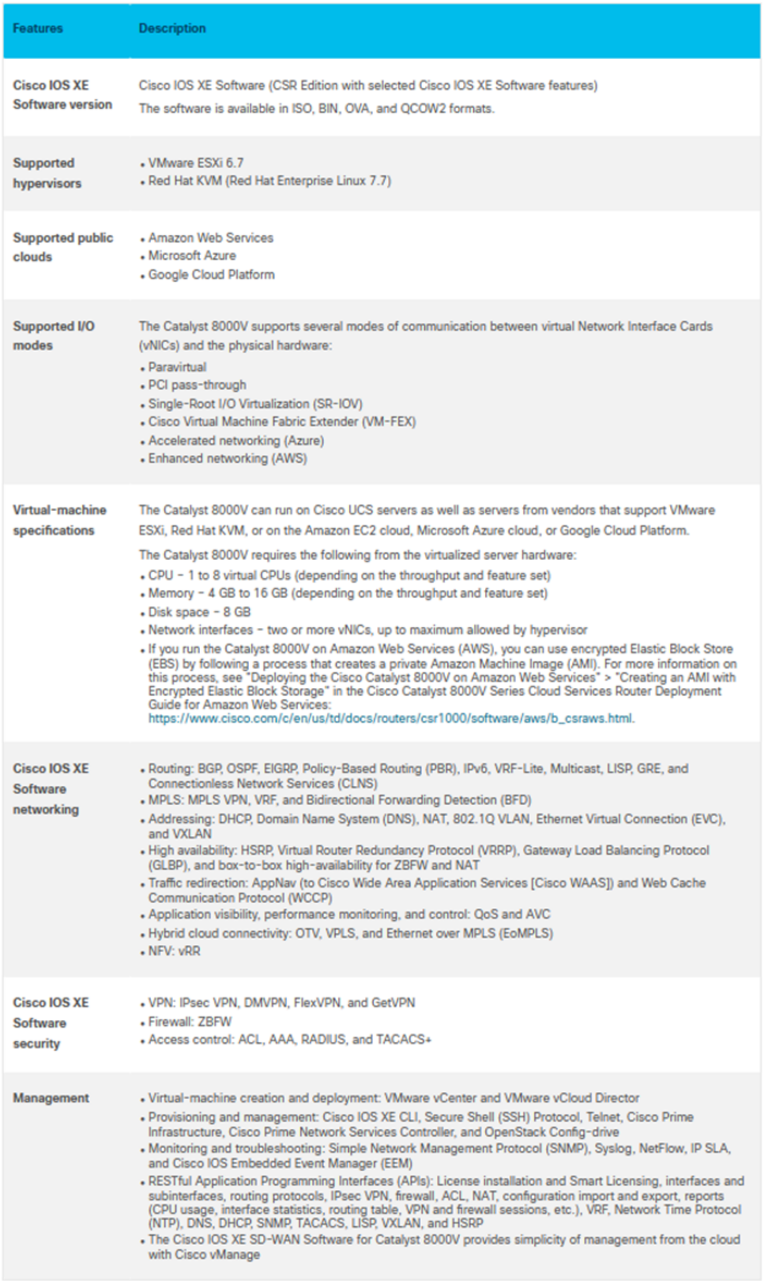
Cisco Catalyst 1000 Series Switches



	Feature	Cisco Catalyst 2960-Plus Series	Cisco Catalyst 2960-L Series	Cisco Catalyst 1000 Series	Benefit
Scale and performance	Downlink type	Fast Ethernet	Gigabit Ethernet	Gigabit Ethernet / Fast Ethernet	Gigabit Ethernet models provide more power and throughput to meet growing demands for connectivity from a wider array of smart devices. Fast Ethernet models support legacy cable infrastructure
	Uplinks	2x 1G, 2x 1000BASE-T	2x 1G, 4x 1G, 4x 10G	2x 1G/Combo**, 4x 1G, 4x 10G 4x 1G/Combo**	
	Maximum PoE budget	Up to 370W	Up to 370W	Up to 740W	
	Perpetual PoE	–	✓	✓	
Flexibility	Operating temperature	Up to 45°C (113°F)	Up to 45°C (113°F)	Up to 50°C (122°F)***	Greater flexibility to allow for more deployment scenarios.
	Single IP management	-	-	✓****	
	Fanless*	-	✓	✓	Increased options for network setup mean you can allocate resources in different ways as your organization and network grows.
	Over-the-air Bluetooth	-	✓	✓	
Functionality	Dynamic VLAN assignment	-	✓	✓	Increased support for VLANs and more advanced quality of service help keep networks secure while meeting multiple requirements for connectivity.
	DHCP relay and server	-	✓	✓	

Specifications Appliances & Software (Continued)

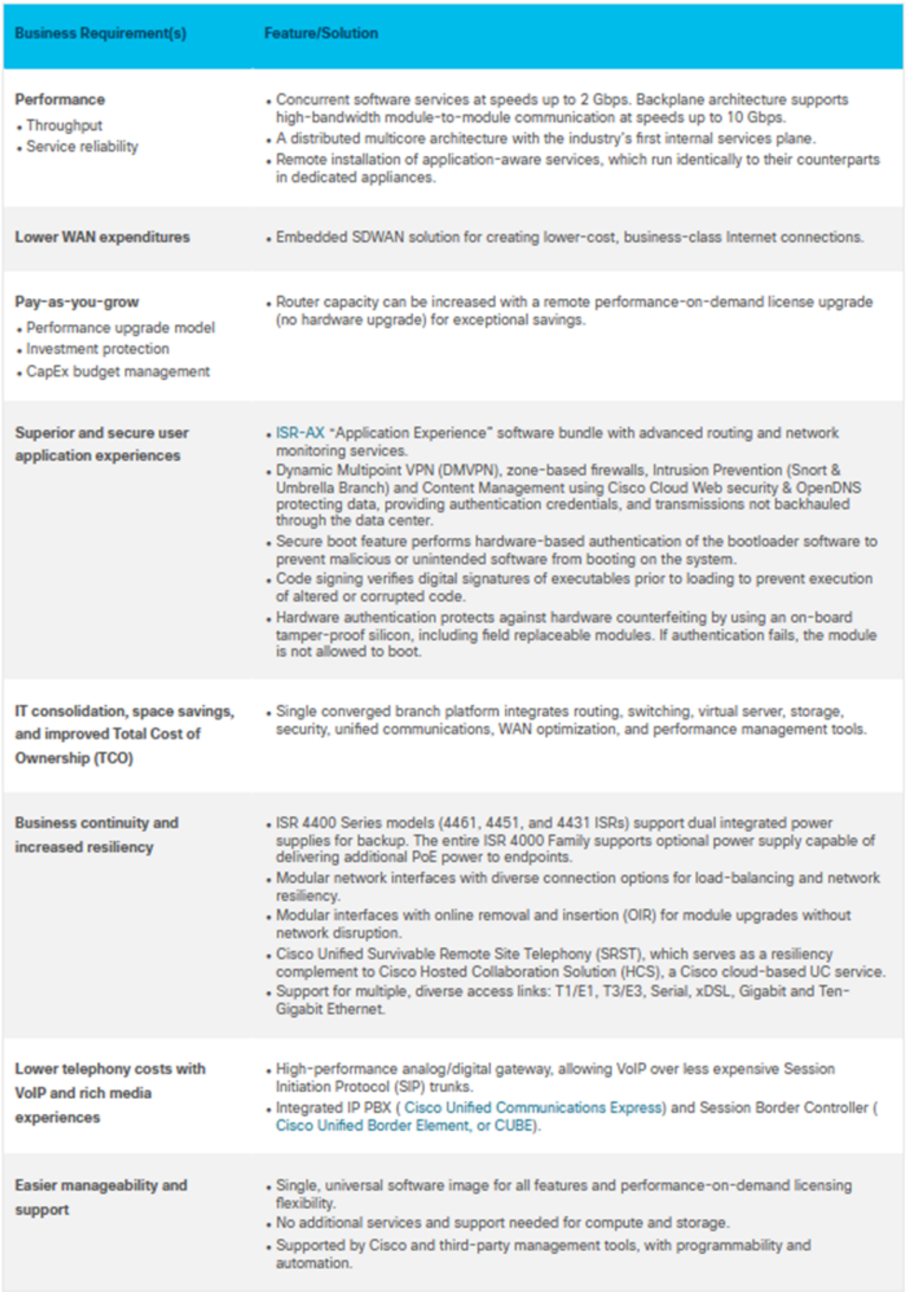
Cisco Catalyst 8000V Edge Software Data



Features	Description
Cisco IOS XE Software version	Cisco IOS XE Software (CSR Edition with selected Cisco IOS XE Software features) The software is available in ISO, BIN, OVA, and QCOW2 formats.
Supported hypervisors	• VMware ESXi 6.7 • Red Hat KVM (Red Hat Enterprise Linux 7.7)
Supported public clouds	• Amazon Web Services • Microsoft Azure • Google Cloud Platform
Supported I/O modes	The Catalyst 8000V supports several modes of communication between virtual Network Interface Cards (vNICs) and the physical hardware: • Paravirtual • PCI pass-through • Single-Root I/O Virtualization (SR-IOV) • Cisco Virtual Machine Fabric Extender (VM-FEX) • Accelerated networking (Azure) • Enhanced networking (AWS)
Virtual-machine specifications	The Catalyst 8000V can run on Cisco UCS servers as well as servers from vendors that support VMware ESXi, Red Hat KVM, or on the Amazon EC2 cloud, Microsoft Azure cloud, or Google Cloud Platform. The Catalyst 8000V requires the following from the virtualized server hardware: • CPU - 1 to 8 virtual CPUs (depending on the throughput and feature set) • Memory - 4 GB to 16 GB (depending on the throughput and feature set) • Disk space - 8 GB • Network interfaces - two or more vNICs, up to maximum allowed by hypervisor • If you run the Catalyst 8000V on Amazon Web Services (AWS), you can use encrypted Elastic Block Store (EBS) by following a process that creates a private Amazon Machine Image (AMI). For more information on this process, see "Deploying the Cisco Catalyst 8000V on Amazon Web Services" > "Creating an AMI with Encrypted Elastic Block Storage" in the Cisco Catalyst 8000V Series Cloud Services Router Deployment Guide for Amazon Web Services: https://www.cisco.com/c/en/us/td/docs/routers/csr1000/software/aws/b_csraws.html.
Cisco IOS XE Software networking	• Routing: BGP, OSPF, EIGRP, Policy-Based Routing (PBR), IPv6, VRF-Lite, Multicast, LISP, GRE, and Connectionless Network Services (CLNS) • MPLS: MPLS VPN, VRF, and Bidirectional Forwarding Detection (BFD) • Addressing: DHCP, Domain Name System (DNS), NAT, 802.1Q VLAN, Ethernet Virtual Connection (EVC), and VXLAN • High availability: HSRP, Virtual Router Redundancy Protocol (VRRP), Gateway Load Balancing Protocol (GLBP), and box-to-box high-availability for ZBFW and NAT • Traffic redirection: AppNav (to Cisco Wide Area Application Services [Cisco WAAS]) and Web Cache Communication Protocol (WCCP) • Application visibility, performance monitoring, and control: QoS and AVC • Hybrid cloud connectivity: OTV, VPLS, and Ethernet over MPLS (EoMPLS) • NFV: vRR
Cisco IOS XE Software security	• VPN: IPsec VPN, DMVPN, FlexVPN, and GetVPN • Firewall: ZBFW • Access control: ACL, AAA, RADIUS, and TACACS+
Management	• Virtual-machine creation and deployment: VMware vCenter and VMware vCloud Director • Provisioning and management: Cisco IOS XE CLI, Secure Shell (SSH) Protocol, Telnet, Cisco Prime Infrastructure, Cisco Prime Network Services Controller, and OpenStack Config-drive • Monitoring and troubleshooting: Simple Network Management Protocol (SNMP), Syslog, NetFlow, IP SLA, and Cisco IOS Embedded Event Manager (EEM) • RESTful Application Programming Interfaces (APIs): License installation and Smart Licensing, interfaces and subinterfaces, routing protocols, IPsec VPN, firewall, ACL, NAT, configuration import and export, reports (CPU usage, interface statistics, routing table, VPN and firewall sessions, etc.), VRF, Network Time Protocol (NTP), DNS, DHCP, SNMP, TACACS, LISP, VXLAN, and HSRP • The Cisco IOS XE SD-WAN Software for Catalyst 8000V provides simplicity of management from the cloud with Cisco vManage

Specifications Appliances & Software (Continued)

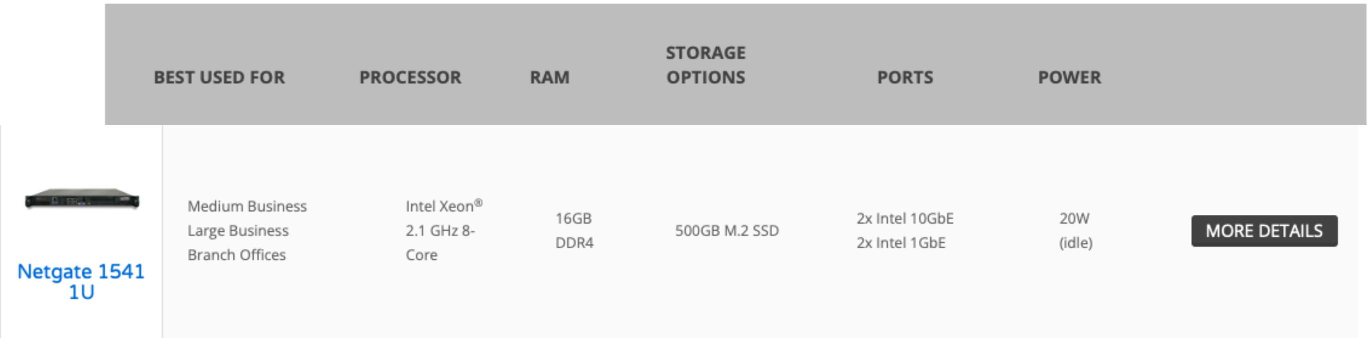
Cisco 4000 Family Integrated Services Router



Business Requirement(s)	Feature/Solution
Performance • Throughput • Service reliability	• Concurrent software services at speeds up to 2 Gbps. Backplane architecture supports high-bandwidth module-to-module communication at speeds up to 10 Gbps. • A distributed multicore architecture with the industry's first internal services plane. • Remote installation of application-aware services, which run identically to their counterparts in dedicated appliances.
Lower WAN expenditures	• Embedded SDWAN solution for creating lower-cost, business-class Internet connections.
Pay-as-you-grow • Performance upgrade model • Investment protection • CapEx budget management	• Router capacity can be increased with a remote performance-on-demand license upgrade (no hardware upgrade) for exceptional savings.
Superior and secure user application experiences	• ISR-AX "Application Experience" software bundle with advanced routing and network monitoring services. • Dynamic Multipoint VPN (DMVPN), zone-based firewalls, Intrusion Prevention (Snort & Umbrella Branch) and Content Management using Cisco Cloud Web security & OpenDNS protecting data, providing authentication credentials, and transmissions not backhauled through the data center. • Secure boot feature performs hardware-based authentication of the bootloader software to prevent malicious or unintended software from booting on the system. • Code signing verifies digital signatures of executables prior to loading to prevent execution of altered or corrupted code. • Hardware authentication protects against hardware counterfeiting by using an on-board tamper-proof silicon, including field replaceable modules. If authentication fails, the module is not allowed to boot.
IT consolidation, space savings, and improved Total Cost of Ownership (TCO)	• Single converged branch platform integrates routing, switching, virtual server, storage, security, unified communications, WAN optimization, and performance management tools.
Business continuity and increased resiliency	• ISR 4400 Series models (4461, 4451, and 4431 ISRs) support dual integrated power supplies for backup. The entire ISR 4000 Family supports optional power supply capable of delivering additional PoE power to endpoints. • Modular network interfaces with diverse connection options for load-balancing and network resiliency. • Modular interfaces with online removal and insertion (OIR) for module upgrades without network disruption. • Cisco Unified Survivable Remote Site Telephony (SRST), which serves as a resiliency complement to Cisco Hosted Collaboration Solution (HCS), a Cisco cloud-based UC service. • Support for multiple, diverse access links: T1/E1, T3/E3, Serial, xDSL, Gigabit and Ten-Gigabit Ethernet.
Lower telephony costs with VoIP and rich media experiences	• High-performance analog/digital gateway, allowing VoIP over less expensive Session Initiation Protocol (SIP) trunks. • Integrated IP PBX (Cisco Unified Communications Express) and Session Border Controller (Cisco Unified Border Element, or CUBE).
Easier manageability and support	• Single, universal software image for all features and performance-on-demand licensing flexibility. • No additional services and support needed for compute and storage. • Supported by Cisco and third-party management tools, with programmability and automation.

Specifications Appliances & Software (Continued)

Netgate 1541 BASE pfSenese + Security Gateway.



	BEST USED FOR	PROCESSOR	RAM	STORAGE OPTIONS	PORTS	POWER	
Netgate 1541 1U	Medium Business Large Business Branch Offices	Intel Xeon® 2.1 GHz 8-Core	16GB DDR4	500GB M.2 SSD	2x Intel 10GbE 2x Intel 1GbE	20W (idle)	MORE DETAILS

Bibliography

About The Author admin. (2021, June 27). *7 steps to create effective IT disaster recovery plan (DRP) & incident response (IR) plan*. ZCyber Security. Retrieved December 8, 2021, from https://zcybersecurity.com/create-disaster-recovery-plan-incident-response-plan/.

Aczechowski. (n.d.). *Security and privacy for apps - configuration manager*. Security and privacy for apps - Configuration Manager | Microsoft Docs. Retrieved December 8, 2021, from https://docs.microsoft.com/en-us/mem/configmgr/apps/plan-design/security-and-privacy-for-application-management.

Burns, B., Killion, D., Beauchesne, N., Moret, E., Sobrier, J., Lynn, M., Markham, E., Iezzoni, C., Biondi, P., Granick, J. S., Manzuik, S., & Guersch, P. (n.d.). *Security Power Tools*. O'Reilly Online Learning. Retrieved December 8, 2021, from https://www.oreilly.com/library/view/security-power-tools/9780596009632/ch14.html#:~:text=Host%20Hardening%20What%20exactly%20do%20we%20mean%20by,or%20by%20enforcing%20authentication%20to%20use%20a%20service.

Citrix Systems, Inc. (2021). *What is access control? - citrix*. Citrix.com. Retrieved December 9, 2021, from https://www.citrix.com/solutions/secure-access/what-is-access-control.html.

Crocetti, P., Peterson, S., & Hefner, K. (2021, February 19). *What is data protection and why is it important? definition from whatis.com*. SearchDataBackup. Retrieved December 8, 2021, from https://searchdatabackup.techtarget.com/definition/data-protection.

Disaster recovery plan (DRP). Disaster Recovery Plan (DRP) - CIO Wiki. (n.d.). Retrieved December 8, 2021, from https://cio-wiki.org/wiki/Disaster_Recovery_Plan_(DRP)#:~:text=Disaster%20Recovery%20Plan%20%28DRP%29%201%20Limit%20the%20magnitude,an%20organized%20and%20effective%20manner.%20More%20items...%20.

Disaster recovery plan (DRP). Disaster Recovery Plan (DRP) - CIO Wiki. (n.d.). Retrieved December 8, 2021, from https://cio-wiki.org/wiki/Disaster_Recovery_Plan_(DRP)#:~:text=Disaster%20Recovery%20Plan%20%28DRP%29%201%20Limit%20the%20magnitude,an%20organized%20and%20effective%20manner.%20More%20items...%20.

Electric Sheep Fencing, LLC. (2021). Learn about the PFSENSE project. Retrieved December 9, 2021, from https://www.pfsense.org/about-pfsense/.

Fortinet, Inc. (2021). *Snort-network intrusion detection and prevention system*. Fortinet. Retrieved December 9, 2021, from https://www.fortinet.com/resources/cyberglossary/snort.

Gegick , M., & Barnum, S. (2005, September 14). *Least privilege*. CISA. Retrieved December 9, 2021, from https://us-cert.cisa.gov/bsi/articles/knowledge/principles/least-privilege.

Hunter, A. (2021, June 1). *What is a domain controller, and why would I need it?* Parallels Remote Application Server Blog - Application virtualization, mobility and VDI. Retrieved December 8, 2021, from https://www.parallels.com/blogs/ras/domain-controller/.

Incident response plan phases. EC. (2021, March 26). Retrieved December 8, 2021, from https://www.eccouncil.org/incident-response-plan-phases/.

Miller, B. (2020, January 24). *15 advantages and disadvantages of Star Topology*. Green Garage. Retrieved December 8, 2021, from https://greengarageblog.org/15-advantages-and-disadvantages-of-star-topology.

Netgate 1541 base pfsense+ security gateway. Netgate. (2021). Retrieved December 9, 2021, from https://shop.netgate.com/products/1541-base-pfsense.

Ot, A., & Anina Ot (86 Articles Published) . (2021, February 3). *6 reasons why you should be using pfsense Firewall*. MUO. Retrieved December 9, 2021, from https://www.makeuseof.com/reasons-use-pfsense-firewall/.

Palo Alto Networks. (2021). *What is an intrusion detection system?* Palo Alto Networks. Retrieved December 9, 2021, from https://www.paloaltonetworks.com/cyberpedia/what-is-an-intrusion-detection-system-ids.

Scarfone, K., & Hoffman, P. (2009, September). Guidelines on Firewalls and Firewall Policy. Gaithersburg, MD; The National Institute of Standards and Technology.

Snort 3 is available! Snort. (2021). Retrieved December 9, 2021, from https://www.snort.org/.

System hardening guidelines for 2022: Critical best practices. Hysolate. (2021, December 5). Retrieved December 8, 2021, from https://www.hysolate.com/blog/system-hardening-guidelines-best-practices/.

Yogesh Chauhan. (n.d.). *What is host hardening and what are some important hardening steps?* Yogesh Chauhan. Retrieved December 8, 2021, from https://yogeshchauhan.com/what-is-host-hardening-and-what-are-some-important-hardening-steps/.