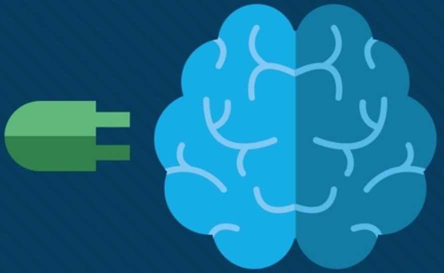


Module 16: Network Security Fundamentals

Introduction to Networks v7.0
(ITN)

Module Objectives

Module Title: Network Security Fundamentals

Module Objective: Configure switches and routers with device hardening features to enhance security.

Topic Title	Topic Objective
Security Threats and Vulnerabilities	Explain why basic security measure are necessary on network devices.
Network Attacks	Identify security vulnerabilities.
Network Attack Mitigation	Identify general mitigation techniques.
Device Security	Configure network devices with device hardening features to mitigate security threats.

16.1 Security Threats and Vulnerabilities

Security Threats and Vulnerabilities

Types of Threats

Attacks on a network can be devastating and can result in a **loss of time and money due to damage, or theft of important information or assets**. Intruders can gain access to a network through software vulnerabilities, hardware attacks, or through guessing someone's username and password. Intruders who gain access by modifying software or exploiting software vulnerabilities are called threat actors.

After the threat actor gains access to the network, four types of threats may arise:

- Information Theft
- Data Loss and manipulation
- Identity Theft
- Disruption of Service

Types of Vulnerabilities

Vulnerability is the degree of **weakness in a network or a device**. Some degree of vulnerability is inherent in routers, switches, desktops, servers, and even security devices. Typically, the network devices under attack are the endpoints, such as servers and desktop computers.

There are three primary vulnerabilities or weaknesses:

- **Technological Vulnerabilities** might include TCP/IP Protocol weaknesses, Operating System Weaknesses, and Network Equipment weaknesses.
- **Configuration Vulnerabilities** might include unsecured user accounts, system accounts with easily guessed passwords, misconfigured internet services, unsecure default settings, and misconfigured network equipment.
- **Security Policy Vulnerabilities** might include lack of a written security policy, politics, lack of authentication continuity, logical access controls not applied, software and hardware installation and changes not following policy, and a nonexistent disaster recovery plan.

All three of these sources of vulnerabilities can leave a network or device open to various attacks, including malicious code attacks and network attacks.

Security Threats and Vulnerabilities

Physical Security

If network resources can be physically compromised, a threat actor can deny the use of network resources. The four classes of physical threats are as follows:

- **Hardware threats -** This includes physical damage to servers, routers, switches, cabling plant, and workstations.
- **Environmental threats -** This includes temperature extremes (too hot or too cold) or humidity extremes (too wet or too dry).
- **Electrical threats -** This includes voltage spikes, insufficient supply voltage (brownouts), unconditioned power (noise), and total power loss.
- **Maintenance threats -** This includes poor handling of key electrical components (electrostatic discharge), lack of critical spare parts, poor cabling, and poor labeling.

A good plan for physical security must be created and implemented to address these issues.

16.2 Network Attacks

Types of Malware

Malware is short for **malicious software**. It is code or software specifically designed to damage, disrupt, steal, or inflict “bad” or illegitimate action on data, hosts, or networks. The following are types of malware:

- **Viruses -** A computer virus is a type of malware that propagates by inserting a copy of itself into, and becoming part of, another program. It spreads from one computer to another, leaving infections as it travels.
- **Worms -** Computer worms are similar to viruses in that they replicate functional copies of themselves and can cause the same type of damage. In contrast to viruses, which require the spreading of an infected host file, worms are standalone software and do not require a host program or human help to propagate.
- **Trojan Horses -** It is a harmful piece of software that looks legitimate. Unlike viruses and worms, Trojan horses do not reproduce by infecting other files. They self-replicate. Trojan horses must spread through user interaction such as opening an email attachment or downloading and running a file from the internet.

Network Attacks

In addition to malicious code attacks, it is also possible for networks to fall prey to various network attacks. Network attacks can be classified into three major categories:

- **Reconnaissance attacks »** - The discovery and mapping of systems, services, or vulnerabilities.
- **Access attacks »** - The unauthorized manipulation of data, system access, or user privileges.
- **Denial of service »** - The disabling or corruption of networks, systems, or services.

Network Attacks

Reconnaissance Attacks

For reconnaissance attacks, external threat actors can use internet tools, such as the **nslookup** and **whois** utilities, to easily determine the IP address space assigned to a given corporation or entity.

After the IP address space is determined, a threat actor can then ping the publicly available IP addresses to identify the addresses that are active.

```
220.128.235.XXX - - [26/Aug/2010:03:00:09 +0200] "GET /db/db/main.php HTTP/1.0" 404 - "-" "-"
220.128.235.XXX - - [26/Aug/2010:03:00:09 +0200] "GET /db/myadmin/main.php HTTP/1.0" 404 - "-" "-"
220.128.235.XXX - - [26/Aug/2010:03:00:10 +0200] "GET /db/webadmin/main.php HTTP/1.0" 404 - "-" "-"
220.128.235.XXX - - [26/Aug/2010:03:00:10 +0200] "GET /db/dbweb/main.php HTTP/1.0" 404 - "-" "-"
220.128.235.XXX - - [26/Aug/2010:03:00:11 +0200] "GET /db/websql/main.php HTTP/1.0" 404 - "-" "-"
220.128.235.XXX - - [26/Aug/2010:03:00:11 +0200] "GET /db/webdb/main.php HTTP/1.0" 404 - "-" "-"
220.128.235.XXX - - [26/Aug/2010:03:00:13 +0200] "GET /db/dbadmin/main.php HTTP/1.0" 404 - "-" "-"
220.128.235.XXX - - [26/Aug/2010:03:00:13 +0200] "GET /db/db-admin/main.php HTTP/1.0" 404 - "-" "-"
```

(https://en.wikipedia.org/wiki/Network_Reconnaissance)

Network Attacks

Access Attacks

Access attacks exploit known vulnerabilities in authentication services, FTP services, and web services to gain entry to web accounts, confidential databases, and other sensitive information.

Access attacks can be classified into four types:

- **Password attacks -** Implemented using brute force, trojan horse, and packet sniffers
- **Trust exploitation -** A threat actor uses unauthorized privileges to gain access to a system, possibly compromising the target.
- **Port redirection**: - A threat actor uses a compromised system as a base for attacks against other targets. For example, a threat actor using SSH (port 22) to connect to a compromised host A. Host A is trusted by host B and, therefore, the threat actor can use Telnet (port 23) to access it.
- **Man-in-the middle -** The threat actor is positioned in between two legitimate entities in order to read or modify the data that passes between the two parties.

Denial of Service Attacks

Denial of service (DoS) attacks are the most publicized form of attack and among the most difficult to eliminate. However, because of their ease of implementation and potentially significant damage, DoS attacks deserve special attention from security administrators.

- DoS attacks take many forms. Ultimately, they prevent authorized people from using a service by **consuming system resources**. To help prevent DoS attacks it is important to stay up to date with the latest security updates for operating systems and applications.
- DoS attacks are a major risk because they interrupt communication and cause significant **loss of time and money**. These attacks are relatively **simple to conduct**, even by an unskilled threat actor.
- A **DDoS** is similar to a DoS attack, but it originates from multiple, coordinated sources. For example, a threat actor builds a network of infected hosts, known as zombies. A network of zombies is called a **botnet**. The threat actor uses a **command and control (CnC) program** to instruct the botnet of zombies to carry out a DDoS attack.

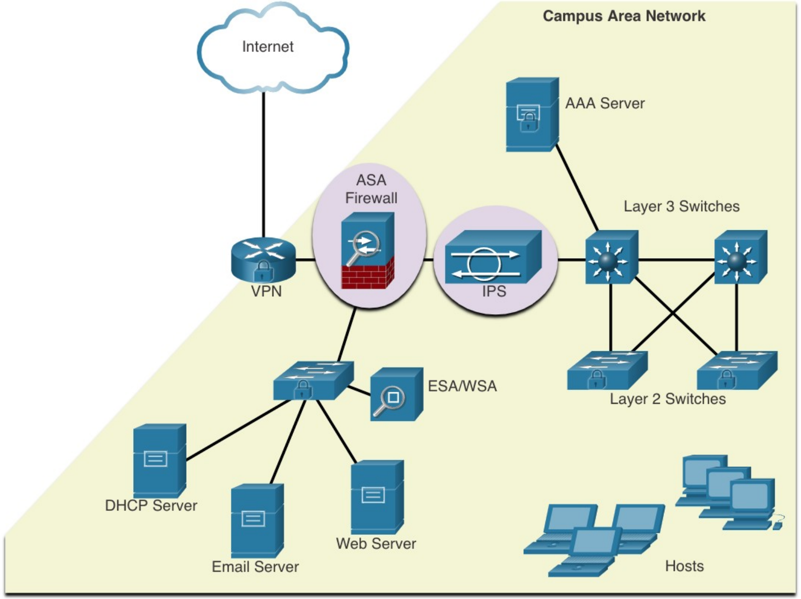
16.3 Network Attack Mitigations

The Defense-in-Depth Approach

To mitigate network attacks, you must first **secure devices including routers, switches, servers, and hosts**. Most organizations employ a defense-in-depth approach (also known as a **layered approach**) to security. This requires a combination of networking devices and services working in tandem.

Several security devices and services are implemented to protect an organization's users and assets against TCP/IP threats:

- VPN
- ASA Firewall
- IPS
- Email Security Appliance (ESA), Web Security Appliance (WSA)
- AAA Server



Network Attack Mitigations
Keep Backups

Backing up device configurations and data is one of the most effective ways of **protecting against data loss**. Backups should be performed on a **regular basis** as identified in the security policy. Data backups are usually **stored offsite** to protect the backup media if anything happens to the main facility.

The table shows backup considerations and their descriptions.

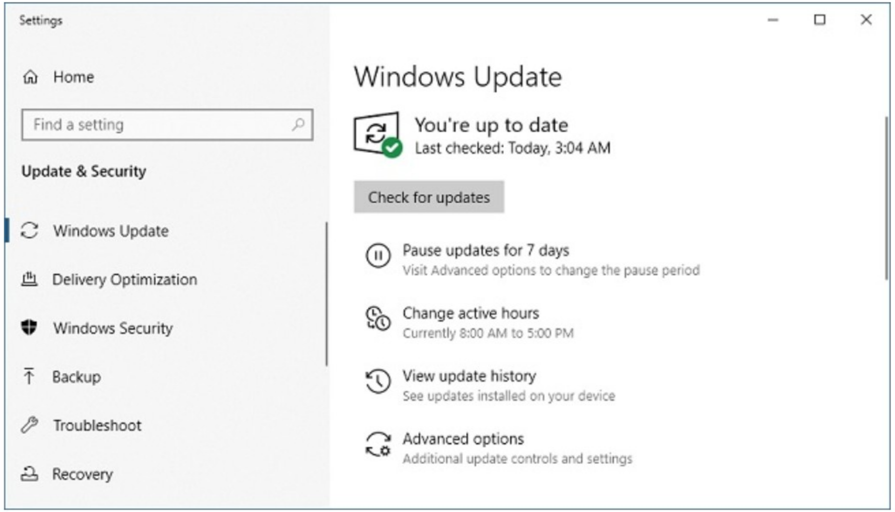
Consideration	Description
Frequency	•Perform backups on a regular basis as identified in the security policy. •Full backups can be time-consuming, therefore perform monthly or weekly backups with frequent partial backups of changed files.
Storage	•Always validate backups to ensure the integrity of the data and validate the file restoration procedures.
Security	•Backups should be transported to an approved offsite storage location on a daily, weekly, or monthly rotation, as required by the security policy.
Validation	•Backups should be protected using strong passwords. The password is required to restore the data.

Network Attack Mitigations

Upgrade, Update, and Patch

As new malware is released, enterprises need to keep current with the **latest versions** of software.

- The most effective way to mitigate a worm attack is to download security updates from the operating system vendor and **patch all vulnerable systems**.
- One solution to the management of critical security patches is to make sure all end systems **automatically download updates**.



Windows Update

You're up to date
Last checked: Today, 3:04 AM

Pause updates for 7 days
Visit Advanced options to change the pause period

Change active hours
Currently 8:00 AM to 5:00 PM

View update history
See updates installed on your device

Advanced options
Additional update controls and settings

Network Attack Mitigations

Authentication, Authorization, and Accounting

Authentication, authorization, and accounting (AAA, or “triple A”) network security services provide the primary framework to set up access control on network devices.

- AAA is a way to control
  - **who is permitted to access a network (authenticate),**
  - **what actions they perform while accessing the network (authorize),**
  - **making a record of what was done while they are there (accounting)**.

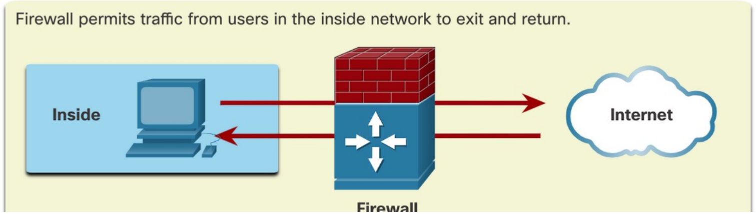
Network Attack Mitigations

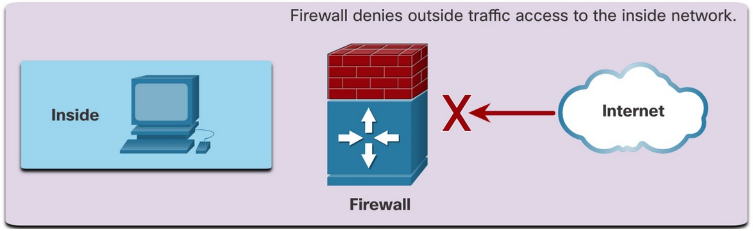
Firewalls

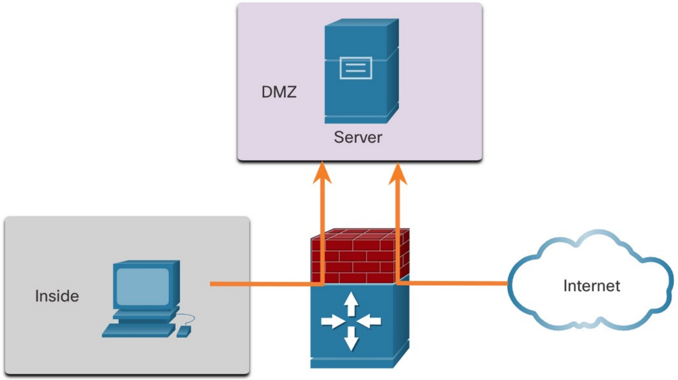
Network firewalls reside **between two or more networks**, control the traffic between them, and help prevent unauthorized access.

A firewall could allow outside users **controlled access to specific services**.

- For example, servers accessible to outside users are usually located on a special network referred to as the **demilitarized zone (DMZ)**.
- The **DMZ** enables a network administrator to apply **specific policies** for hosts connected to that network.


Firewall permits traffic from users in the inside network to exit and return.


Firewall denies outside traffic access to the inside network.



Network Attack Mitigations

Types of Firewalls

Firewall products come packaged in various forms. These products use different techniques for determining what will be permitted or denied access to a network. They include the following:

- **Packet filtering** - Prevents or allows access based on IP or MAC addresses
- **Application filtering** - Prevents or allows access by specific application types based on port numbers
- **URL filtering** - Prevents or allows access to websites based on specific URLs or keywords
- **Stateful packet inspection (SPI)** - Incoming packets must be legitimate responses to requests from internal hosts. Unsolicited packets are blocked unless permitted specifically. SPI can also include the capability to recognize and filter out specific types of attacks, such as denial of service (DoS).

Network Attack Mitigations
Endpoint Security

An endpoint, or host, is an individual computer system or device that acts as a network client. Common endpoints are laptops, desktops, servers, smartphones, and tablets.

Securing endpoint devices is one of the most challenging jobs of a network administrator because it involves human nature. A company must have **well-documented policies in place and employees must be aware of these rules**.

Employees need to be trained on proper use of the network. Policies often include the use of antivirus software and host intrusion prevention. More comprehensive endpoint security solutions rely on network access control.

16.4 Device Security

Device Security

There are some simple steps that should be taken that apply to most operating systems:

- **Default usernames and passwords should be changed immediately.**
- **Access** to system resources should be **restricted** to only the individuals that are authorized to use those resources.
- Any **unnecessary services and applications** should be **turned off** and uninstalled when possible.
- Often, devices shipped from the manufacturer have been sitting in a warehouse for a period of time and do not have the most up-to-date patches installed. It is important to **update any software** and install any security patches prior to implementation.

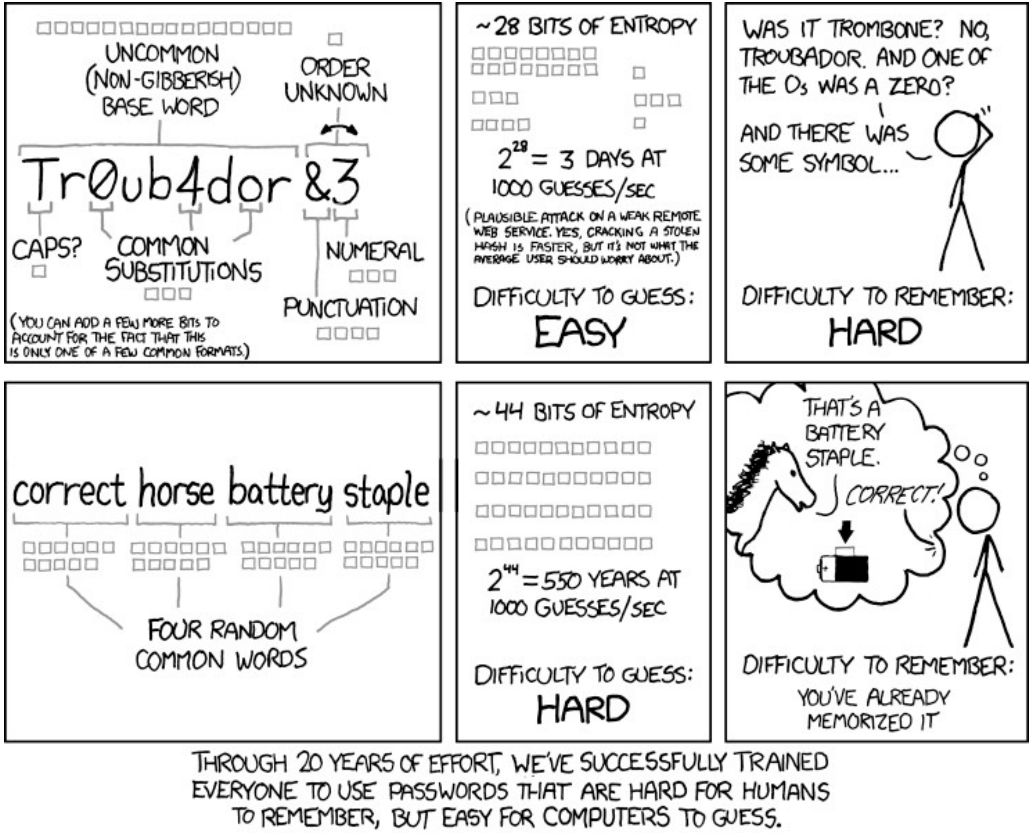
Device Security

Passwords

To protect network devices, it is important to use strong passwords. Here are standard guidelines to follow:

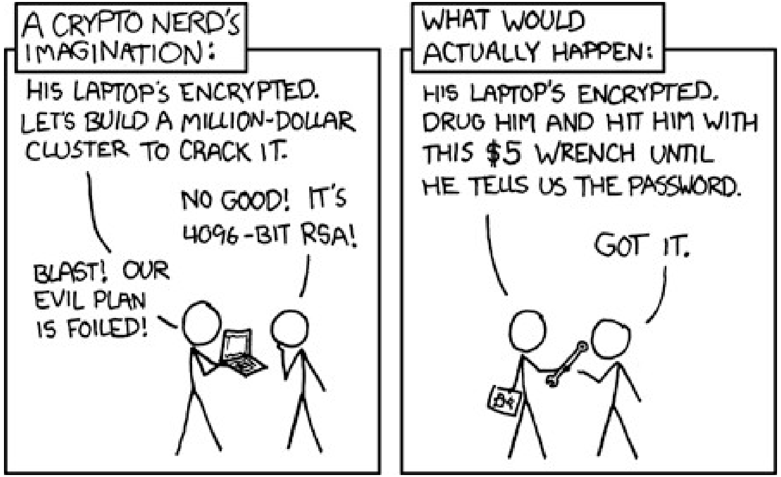
- Use a password length of at least eight characters, preferably 10 or more characters.
- Make passwords complex. Include a mix of uppercase and lowercase letters, numbers, symbols, and spaces, if allowed.
- Avoid passwords based on repetition, common dictionary words, letter or number sequences, usernames, relative or pet names, biographical information, such as birthdates, ID numbers, ancestor names, or other easily identifiable pieces of information.
- Deliberately misspell a password. For example, Smith = Smyth = 5mYth or Security = 5ecur1ty.
- Change passwords often. If a password is unknowingly compromised, the window of opportunity for the threat actor to use the password is limited.
- Do not write passwords down and leave them in obvious places such as on the desk or monitor.

On Cisco routers, leading spaces are ignored for passwords, but spaces after the first character are not. Therefore, one method to create a strong password is to use the space bar and create a phrase made of many words. This is called a passphrase. A passphrase is often easier to remember than a simple password. It is also longer and harder to guess.


UNCOMMON (NON-GIBBERISH) BASE WORD
ORDER UNKNOWN
Tr0ub4dor &3
CAPS?
COMMON SUBSTITUTIONS
NUMERAL
PUNCTUATION
(YOU CAN ADD A FEW MORE BITS TO ACCOUNT FOR THE FACT THAT THIS IS ONLY ONE OF A FEW COMMON FORMATS.)
~28 BITS OF ENTROPY
2^28 = 3 DAYS AT 1000 GUESSES/SEC
(PLAUSIBLE ATTACK ON A WEAK REMOTE WEB SERVICE. YES, CRACKING A STOLEN HASH IS FASTER, BUT IT'S NOT WHAT THE AVERAGE USER SHOULD WORRY ABOUT.)
DIFFICULTY TO GUESS: EASY
WAS IT TROMBONE? NO, TROUBADOR. AND ONE OF THE Os WAS A ZERO?
AND THERE WAS SOME SYMBOL...
DIFFICULTY TO REMEMBER: HARD
correct horse battery staple
FOUR RANDOM COMMON WORDS
~44 BITS OF ENTROPY
2^44 = 550 YEARS AT 1000 GUESSES/SEC
DIFFICULTY TO GUESS: HARD
THAT'S A BATTERY STAPLE.
CORRECT!
DIFFICULTY TO REMEMBER: YOU'VE ALREADY MEMORIZED IT
THROUGH 20 YEARS OF EFFORT, WE'VE SUCCESSFULLY TRAINED EVERYONE TO USE PASSWORDS THAT ARE HARD FOR HUMANS TO REMEMBER, BUT EASY FOR COMPUTERS TO GUESS.

https://xkcd.com/936/

https://xkcd.com/538/

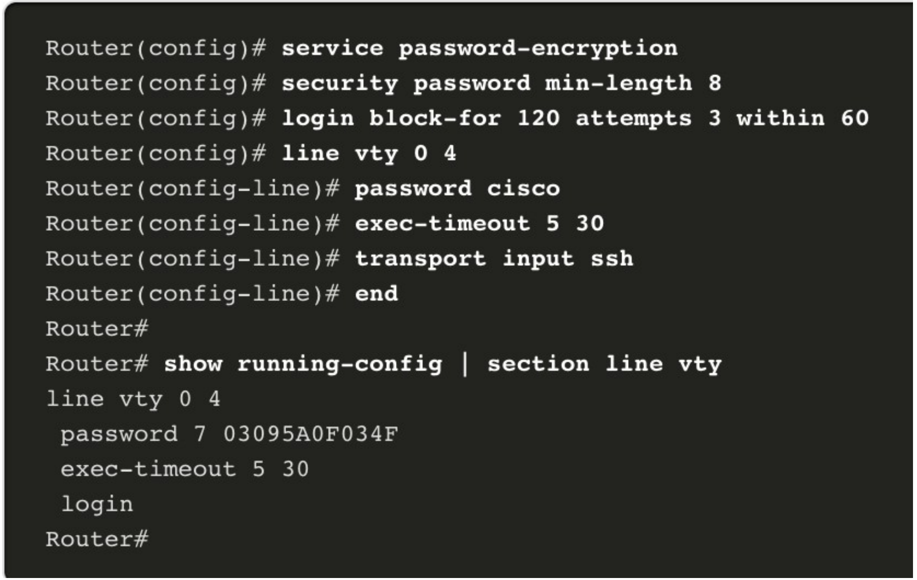

A CRYPTO NERD'S IMAGINATION:
HIS LAPTOP'S ENCRYPTED. LET'S BUILD A MILLION-DOLLAR CLUSTER TO CRACK IT.
NO GOOD! IT'S 4096-BIT RSA!
BLAST! OUR EVIL PLAN IS FOILED!
WHAT WOULD ACTUALLY HAPPEN:
HIS LAPTOP'S ENCRYPTED. DRUG HIM AND HIT HIM WITH THIS $5 WRENCH UNTIL HE TELLS US THE PASSWORD.
GOT IT.
$4

Device Security

Additional Password Security

There are several steps that can be taken to help ensure that passwords remain secret on a Cisco router and switch including these:

- Encrypt all plaintext passwords with the **service password-encryption** command.
- Set a minimum acceptable password length with the **security passwords min-length** command.
- Deter brute-force password guessing attacks with the **login block-for # attempts # within #** command.
- Disable an inactive privileged EXEC mode access after a specified amount of time with the **exec-timeout** command.



```
Router(config)# service password-encryption
Router(config)# security password min-length 8
Router(config)# login block-for 120 attempts 3 within 60
Router(config)# line vty 0 4
Router(config-line)# password cisco
Router(config-line)# exec-timeout 5 30
Router(config-line)# transport input ssh
Router(config-line)# end
Router#
Router# show running-config | section line vty
line vty 0 4
 password 7 03095A0F034F
 exec-timeout 5 30
 login
Router#
```

Cisco Type 7 Reversers

Enable SSH

It is possible to configure a Cisco device to support SSH using the following steps:

1. **Configure a unique device hostname**. A device must have a unique hostname other than the default.
2. **Configure the IP domain name**. Configure the IP domain name of the network by using the global configuration mode command **ip-domain name**.
3. **Generate a key to encrypt SSH traffic**. SSH encrypts traffic between source and destination. However, to do so, a unique authentication key must be generated by using the global configuration command **crypto key generate rsa general-keys modulus** *bits*. The modulus *bits* determines the size of the key and can be configured from 360 bits to 2048 bits. The larger the bit value, the more secure the key. However, larger bit values also take longer to encrypt and decrypt information. The minimum recommended modulus length is 1024 bits.
4. **Verify or create a local database entry**. Create a local database username entry using the **username** global configuration command.
5. **Authenticate against the local database**. Use the **login local** line configuration command to authenticate the vty line against the local database.
6. **Enable vty inbound SSH sessions**. By default, no input session is allowed on vty lines. You can specify multiple input protocols including Telnet and SSH using the **transport input [ssh | telnet]** command.

Device Security

Disable Unused Services

Cisco routers and switches start with a list of active services that may or may not be required in your network. Disable any unused services to preserve system resources, such as CPU cycles and RAM, and prevent threat actors from exploiting these services.

- The type of services that are on by default will vary depending on the IOS version. For example, IOS-XE typically will have only HTTPS and DHCP ports open. You can verify this with the **show ip ports all** command.
- IOS versions prior to IOS-XE use the **show control-plane host open-ports** command.

Summary

What Did I Learn In This Module?

- After the threat actor gains access to the network, four types of threats may arise: information theft, data loss and manipulation, identity theft, and disruption of service.
- There are three primary vulnerabilities or weaknesses: technological, configuration, and security policy.
- The four classes of physical threats are: hardware, environmental, electrical, and maintenance.
- Malware is short for malicious software. It is code or software specifically designed to damage, disrupt, steal, or inflict “bad” or illegitimate action on data, hosts, or networks. Viruses, worms, and Trojan horses are types of malware.
- Network attacks can be classified into three major categories: reconnaissance, access, and denial of service.
- To mitigate network attacks, you must first secure devices including routers, switches, servers, and hosts. Most organizations employ a defense-in-depth approach to security. This requires a combination of networking devices and services working together.
- Several security devices and services are implemented to protect an organization’s users and assets against TCP/IP threats: VPN, ASA firewall, IPS, ESA/WSA, and AAA server.

Module Practice and Quiz

What Did I Learn In This Module? (Cont.)

- Infrastructure devices should have backups of configuration files and IOS images on an FTP or similar file server. If the computer or a router hardware fails, the data or configuration can be restored using the backup copy.
- The most effective way to mitigate a worm attack is to download security updates from the operating system vendor and patch all vulnerable systems. To manage critical security patches, to make sure all end systems automatically download updates.
- AAA is a way to control who is permitted to access a network (authenticate), what they can do while they are there (authorize), and what actions they perform while accessing the network (accounting).
- Network firewalls reside between two or more networks, control the traffic between them, and help prevent unauthorized access.
- Securing endpoint devices is critical to network security. A company must have well-documented policies in place, which may include the use of antivirus software and host intrusion prevention. More comprehensive endpoint security solutions rely on network access control.

What Did I Learn In This Module? (Cont.)

- For Cisco routers, the Cisco AutoSecure feature can be used to assist securing the system. For most OSs default usernames and passwords should be changed immediately, access to system resources should be restricted to only the individuals that are authorized to use those resources, and any unnecessary services and applications should be turned off and uninstalled when possible.
- To protect network devices, it is important to use strong passwords. A passphrase is often easier to remember than a simple password. It is also longer and harder to guess.
- For routers and switches, encrypt all plaintext passwords, setting a minimum acceptable password length, deter brute-force password guessing attacks, and disable an inactive privileged EXEC mode access after a specified amount of time.
- Configure appropriate devices to support SSH, and disable unused services.

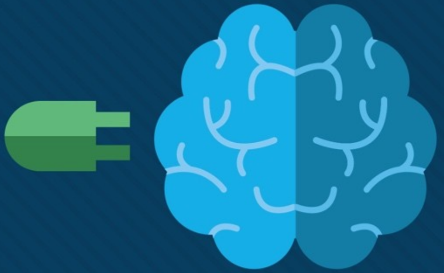
New Terms and Commands

- threat actor
- malware
- reconnaissance attacks
- access attacks
- defense-in-depth
- authentication, authorization, and accounting (AAA)
- demilitarized zone (DMZ)
- Cisco AutoSecure
- passphrase

- **service password-encryption**
- **security passwords min-length**
- **login block-for**
- **exec-timeout**
- **crypto key generate rsa general-keys modulus**
- **username password | secret**
- **login local**
- **transport input ssh**
- **show ip ports all**
- **show control-plan host open-ports**

Module 17: Build a Small Network

Introduction to Networks v7.0
(ITN)



Module Objectives

Module Title: Build a Small Network

Module Objective: Implement a network design for a small network to include a router, a switch, and end devices.

Topic Title	Topic Objective
Devices in a Small Network	Identify the devices used in a small network.
Small Network Applications and Protocols	Identify the protocols and applications used in a small network.
Scale to Larger Networks	Explain how a small network serves as the basis of larger networks.
Verify Connectivity	Use the output of the ping and tracert commands to verify connectivity and establish relative network performance.
Host and IOS Commands	Use host and IOS commands to acquire information about the devices in a network.
Troubleshooting Methodologies	Describe common network troubleshooting methodologies.
Troubleshooting Scenarios	Troubleshoot issues with devices in the network.

17.1 Devices in a Small Network

Devices in a Small Network

Small Network Topologies

- **The majority of businesses are small most of the business networks are also small.**
- A small network design is usually **simple**.
- Small networks typically have a single WAN connection provided by DSL, cable, or an Ethernet connection.
- Large networks require an IT department to maintain, secure, and troubleshoot network devices and to protect organizational data. Small networks are managed by **a local IT technician or by a contracted professional**.

Device Selection for a Small Network

Like large networks, small networks require planning and design to meet user requirements. **Planning ensures that all requirements, cost factors, and deployment options are given due consideration**. One of the first design considerations is the type of intermediary devices to use to support the network.

Factors that must be considered when selecting network devices include:

- cost
- speed and types of ports/interfaces
- expandability
- operating system features and services

IP Addressing for a Small Network

When implementing a network, **create an IP addressing scheme and use it**. All hosts and devices within an internetwork must have a unique address. Devices that will factor into the IP addressing scheme include the following:

- End user devices - The number and type of connections (i.e., wired, wireless, remote access)
- Servers and peripherals devices (e.g., printers and security cameras)
- Intermediary devices including switches and access points

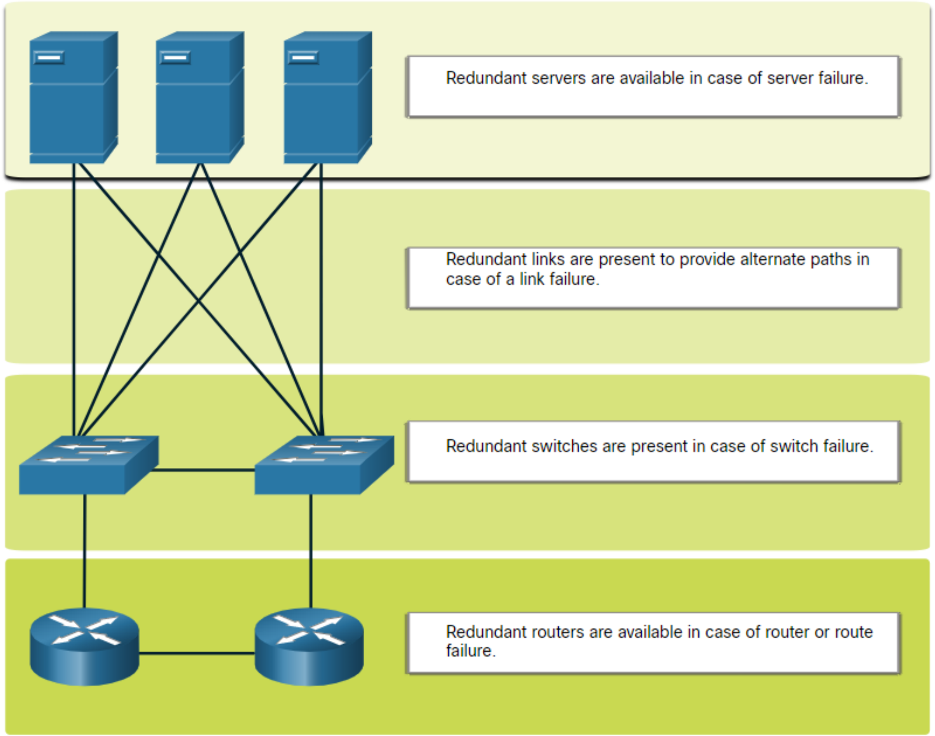
It is recommended that you plan, document, and maintain an IP addressing scheme based on device type. The use of a planned IP addressing scheme makes it easier to identify a type of device and to troubleshoot problems.

Devices in a Small Network

Redundancy in a Small Network

In order to maintain a high degree of reliability, *redundancy* is required in the network design. Redundancy helps to eliminate single points of failure.

Redundancy can be accomplished by installing duplicate equipment. It can also be accomplished by supplying duplicate network links for critical areas.



Redundant servers are available in case of server failure.

Redundant links are present to provide alternate paths in case of a link failure.

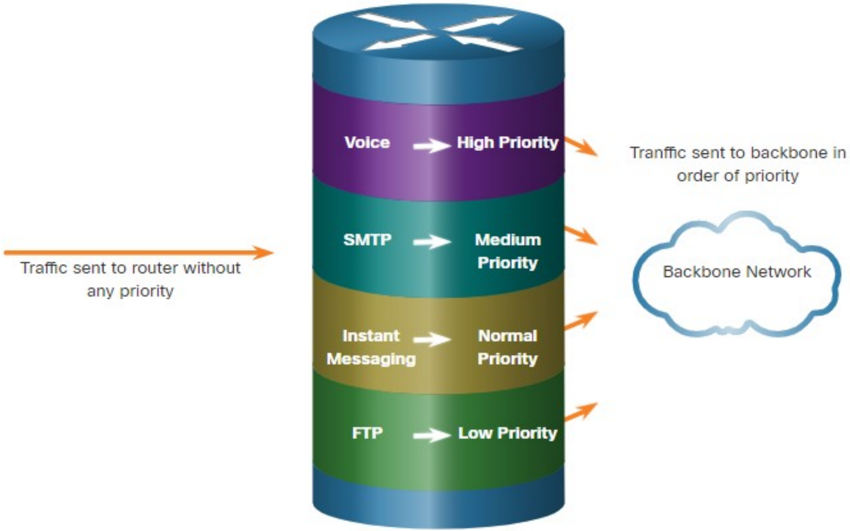
Redundant switches are present in case of switch failure.

Redundant routers are available in case of router or route failure.

Devices in a Small Network

Traffic Management

- The goal for a good network design is to enhance the productivity of the employees and minimize network downtime.
- The routers and switches in a small network should be configured to support real-time traffic, such as voice and video, in an appropriate manner relative to other data traffic. A good network design will implement quality of service (QoS).
- Priority queuing has four queues. The high-priority queue is always emptied first.



17.2 Small Network Applications and Protocols

Common Applications

After you have set it up, your network still needs certain types of applications and protocols in order to work. The network is only as useful as the applications that are on it.

There are two forms of software programs or processes that provide access to the network:

- **Network Applications**: Applications that implement application layer protocols and are able to communicate directly with the lower layers of the protocol stack.
- **Application Layer Services**: For applications that are not network-aware, the programs that interface with the network and prepare the data for transfer.

Small Network Applications and Protocols
Common Protocols

Network protocols support the applications and services used by employees in a small network.

- Network administrators commonly require access to network devices and servers. The two most common remote access solutions are Telnet and Secure Shell (SSH).
- Hypertext Transfer Protocol (HTTP) and Hypertext Transfer Protocol Secure (HTTP) are used between web clients and web servers.
- Simple Mail Transfer Protocol (SMTP) is used to send email, Post Office Protocol (POP3) or Internet Mail Access Protocol (IMAP) are used by clients to retrieve email.
- File Transfer Protocol (FTP) and Security File Transfer Protocol (SFTP) are used to download and upload files between a client and an FTP server.
- Dynamic Host Configuration Protocol (DHCP) is used by clients to acquire an IP configuration from a DHCP Server.
- The Domain Name Service (DNS) resolves domain names to IP addresses.

Note: A server could provide multiple network services. For instance, a server could be an email, FTP and SSH server.

Voice and Video Applications

- Businesses today are increasingly using IP telephony and streaming media to communicate with customers and business partners, as well as enabling their employees to work remotely.
- The network administrator must ensure the proper equipment is installed in the network and that the network devices are configured to ensure priority delivery.
- The factors that a small network administrator must consider when supporting real-time applications:
  - **Infrastructure -** Does it have the capacity and capability to support real-time applications?
  - **VoIP -** VoIP is typically less expensive than IP Telephony, but at the cost of quality and features.
  - **IP Telephony -** This employs dedicated servers form call control and signaling.
  - **Real-Time Applications -** The network must support Quality of Service (QoS) mechanisms to minimize latency issues. Real-Time Transport Protocol (RTP) and Real-Time Transport Control Protocol (RTCP) and two protocols that support real-time applications.

17.3 Scale to Larger Networks

Small Network Growth

Growth is a natural process for many small businesses, and their networks must grow accordingly. Ideally, the network administrator has enough lead-time to make intelligent decisions about growing the network in alignment with the growth of the company.

To scale a network, several elements are required:

- **Network documentation** - Physical and logical topology
- **Device inventory** - List of devices that use or comprise the network
- **Budget** - Itemized IT budget, including fiscal year equipment purchasing budget
- **Traffic analysis** - Protocols, applications, and services and their respective traffic requirements should be documented

These elements are used to inform the decision-making that accompanies the scaling of a small network.

Protocol Analysis

It is important to understand the type of traffic that is crossing the network as well as the current traffic flow. There are several network management tools that can be used for this purpose.

To **determine traffic flow patterns**, it is important to do the following:

- Capture traffic during **peak utilization times** to get a good representation of the different traffic types.
- Perform the capture on different network segments and devices as some traffic will be local to a particular segment.
- Information gathered by the protocol analyzer is evaluated based on the source and destination of the traffic, as well as the type of traffic being sent.
- This analysis can be used to make **decisions on how to manage the traffic more efficiently**.

Scale to Larger Networks

Employee Network Utilization

Many operating systems provide built-in tools to display such network utilization information. These tools can be used to capture a “snapshot” of information such as the following:

- OS and OS Version
- CPU utilization
- RAM utilization
- Drive utilization
- Non-Network applications
- Network applications

Documenting snapshots for employees in a small network over a period of time is very useful to identify evolving protocol requirements and associated traffic flows.

17.4 Verify Connectivity

Network Baseline

- One of the most effective tools for monitoring and troubleshooting network performance is to establish a network baseline.
- One method for **starting a baseline is to copy and paste the results from an executed ping, trace, or other relevant commands into a text file**. These text files can be time stamped with the date and saved into an archive for later retrieval and comparison.
- Among items to consider are error messages and the response times from host to host.
- Corporate networks should have extensive baselines; more extensive than we can describe in this course. Professional-grade software tools are available for storing and maintaining baseline information.

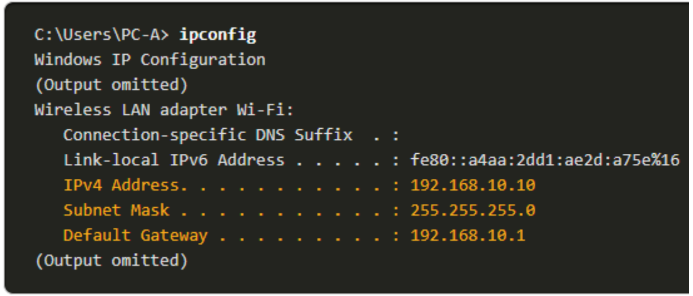
17.5 Host and IOS Commands

Host and IOS Commands

IP Configuration on a Windows Host

In Windows 10, you can access the IP address details from the **Network and Sharing Center** to quickly view the four important settings: address, mask, router, and DNS. Or you can issue the **ipconfig** command at the command line of a Windows computer.

- Use the **ipconfig /all** command to view the MAC address, as well as a number of details regarding the Layer 3 addressing of the device.
- If a host is configured as a DHCP client, the IP address configuration can be renewed using the **ipconfig /release** and **ipconfig /renew** commands.
- The DNS Client service on Windows PCs also optimizes the performance of DNS name resolution by storing previously resolved names in memory. The **ipconfig /displaydns** command displays all of the cached DNS entries on a Windows computer system.



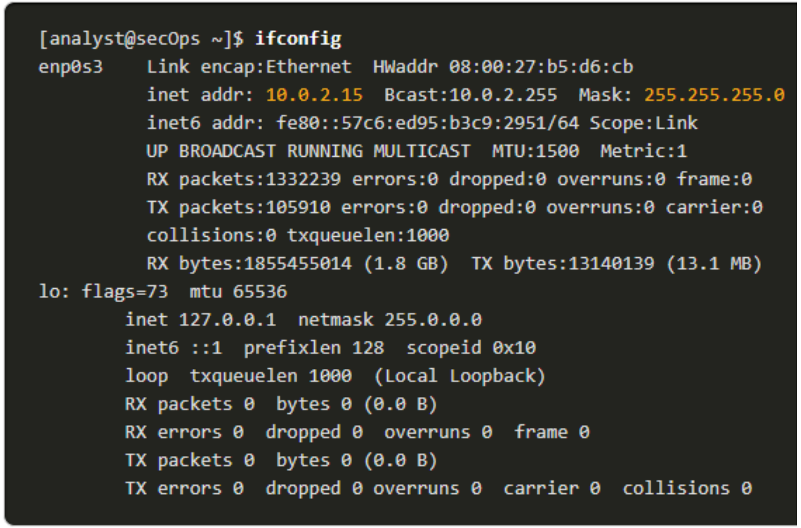
```
C:\Users\PC-A> ipconfig
Windows IP Configuration
(Output omitted)
Wireless LAN adapter Wi-Fi:
   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::a4aa:2dd1:ae2d:a75e%16
   IPv4 Address. . . . . . . . . . . : 192.168.10.10
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.10.1
(Output omitted)
```

Host and IOS Commands

IP Configuration on a Linux Host

- Verifying IP settings using the GUI on a Linux machine will differ depending on the Linux distribution and desktop interface.
- On the command line, use the **ifconfig** command to display the status of the currently active interfaces and their IP configuration.
- The Linux **ip address** command is used to display addresses and their properties. It can also be used to add or delete IP addresses.

Note: The output displayed may vary depending on the Linux distribution.

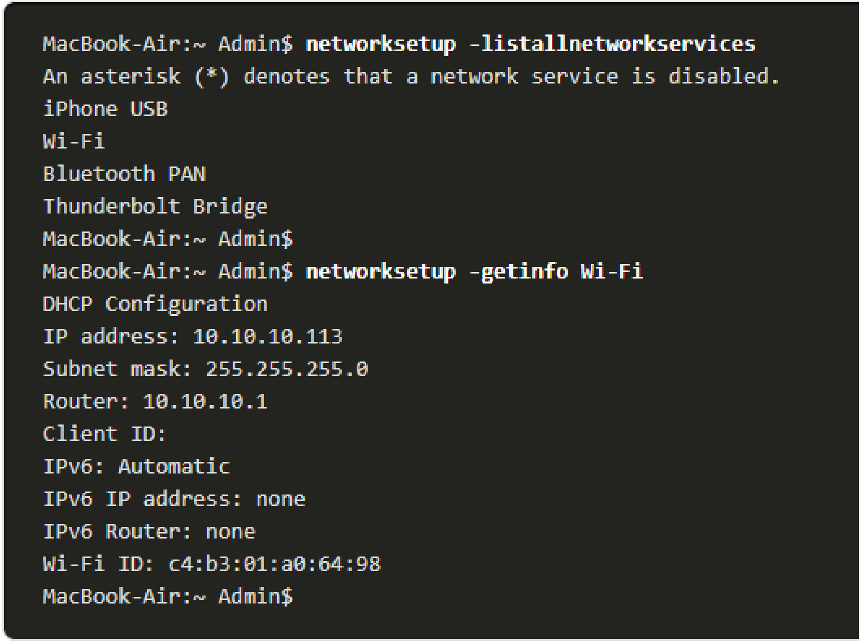


```
[analyst@secOps ~]$ ifconfig
enp0s3     Link encap:Ethernet  HWaddr 08:00:27:b5:d6:cb
           inet addr: 10.0.2.15  Bcast:10.0.2.255  Mask: 255.255.255.0
           inet6 addr: fe80::57c6:ed95:b3c9:2951/64 Scope:Link
           UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
           RX packets:1332239 errors:0 dropped:0 overruns:0 frame:0
           TX packets:105910 errors:0 dropped:0 overruns:0 carrier:0
           collisions:0 txqueuelen:1000
           RX bytes:1855455014 (1.8 GB)  TX bytes:13140139 (13.1 MB)
lo: flags=73  mtu 65536
         inet 127.0.0.1  netmask 255.0.0.0
         inet6 ::1  prefixlen 128  scopeid 0x10
         loop  txqueuelen 1000  (Local Loopback)
         RX packets 0  bytes 0 (0.0 B)
         RX errors 0  dropped 0  overruns 0  frame 0
         TX packets 0  bytes 0 (0.0 B)
         TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Host and IOS Commands

IP Configuration on a macOS Host

- In the GUI of a Mac host, open **Network Preferences > Advanced** to get the IP addressing information.
- The **ifconfig** command can also be used to verify the interface IP configuration at the command line.
- Other useful macOS commands to verify the host IP settings include **networksetup -listallnetworkservices** and the **networksetup -getinfo <***network service***>**.



```
MacBook-Air:~ Admin$ networksetup -listallnetworkservices
An asterisk (*) denotes that a network service is disabled.
iPhone USB
Wi-Fi
Bluetooth PAN
Thunderbolt Bridge
MacBook-Air:~ Admin$
MacBook-Air:~ Admin$ networksetup -getinfo Wi-Fi
DHCP Configuration
IP address: 10.10.10.113
Subnet mask: 255.255.255.0
Router: 10.10.10.1
Client ID:
IPv6: Automatic
IPv6 IP address: none
IPv6 Router: none
Wi-Fi ID: c4:b3:01:a0:64:98
MacBook-Air:~ Admin$
```

The arp Command

The **arp** command is executed from the Windows, Linux, or Mac command prompt. The command lists all devices currently in the ARP cache of the host.

- The **arp -a** command displays the known IP address and MAC address binding. The ARP cache only displays information from devices that have been recently accessed.
- To ensure that the ARP cache is populated, **ping** a device so that it will have an entry in the ARP table.
- The cache can be cleared by using the **netsh interface ip delete arpcache** command in the event the network administrator wants to repopulate the cache with updated information.

Note: You may need administrator access on the host to be able to use the **netsh interface ip delete arpcache** command.

Host and IOS Commands

Common show Commands Revisited

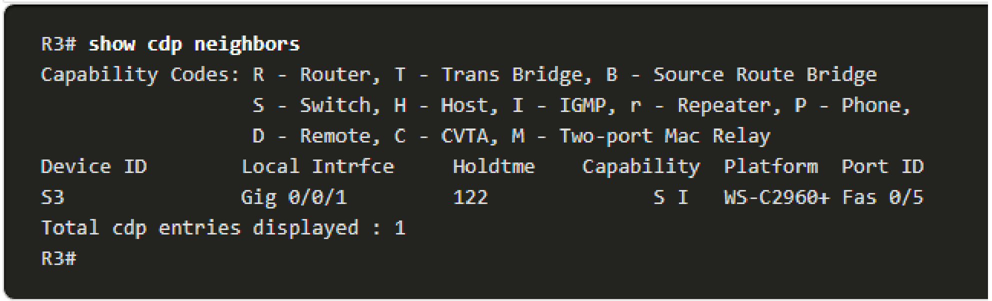
Command	Description
show running-config	Verifies the current configuration and settings
show interfaces	Verifies the interface status and displays any error messages
show ip interface	Verifies the Layer 3 information of an interface
show arp	Verifies the list of known hosts on the local Ethernet LANs
show ip route	Verifies the Layer 3 routing information
show protocols	Verifies which protocols are operational
show version	Verifies the memory, interfaces, and licenses of the device

The show cdp neighbors Command

CDP provides the following information about each CDP neighbor device:

- **Device identifiers** - The configured host name of a switch, router, or other device
- **Address list** - Up to one network layer address for each protocol supported
- **Port identifier** - The name of the local and remote port in the form of an ASCII character string, such as FastEthernet 0/0
- **Capabilities list** - Whether a specific device is a Layer 2 switch or a Layer 3 switch
- **Platform** - The hardware platform of the device.

The **show cdp neighbors detail** command reveals the IP address of a neighboring device.

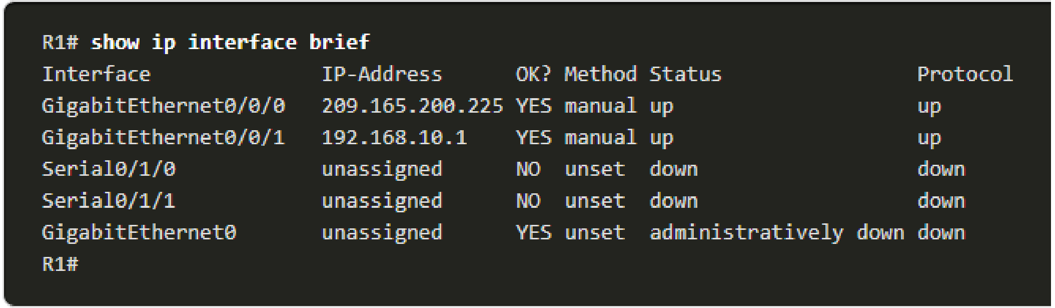


```
R3# show cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone,
                  D - Remote, C - CVTA, M - Two-port Mac Relay
Device ID        Local Intrfce     Holdtme    Capability  Platform  Port ID
S3               Gig 0/0/1         122              S I   WS-C2960+ Fas 0/5
Total cdp entries displayed : 1
R3#
```

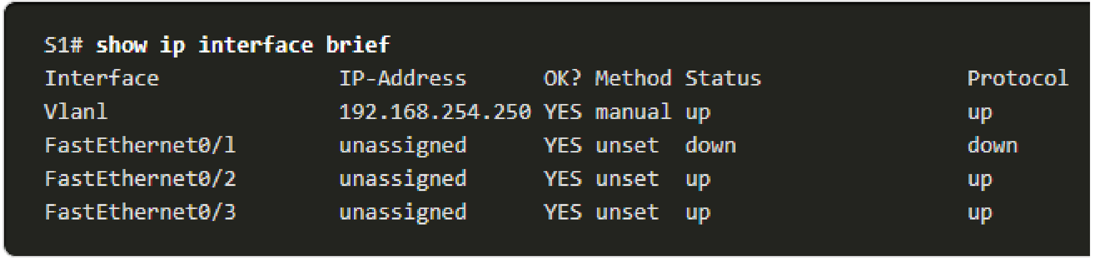
Host and IOS Commands

The show ip interface brief Command

One of the most frequently used commands is the **show ip interface brief** command. This command provides a more abbreviated output than the **show ip interface** command. It provides a summary of the key information for all the network interfaces on a router.



```
R1# show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
GigabitEthernet0/0/0   209.165.200.225 YES manual up                    up
GigabitEthernet0/0/1   192.168.10.1    YES manual up                    up
Serial0/1/0            unassigned      NO  unset  down                  down
Serial0/1/1            unassigned      NO  unset  down                  down
GigabitEthernet0       unassigned      YES unset  administratively down down
R1#
```



```
S1# show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
Vlanl                  192.168.254.250 YES manual up                    up
FastEthernet0/l        unassigned      YES unset  down                  down
FastEthernet0/2        unassigned      YES unset  up                    up
FastEthernet0/3        unassigned      YES unset  up                    up
```

17.6 Troubleshooting Methodologies

Troubleshooting Methodologies

Basic Troubleshooting Approaches

Step	Description
Step 1. Identify the Problem	•This is the first step in the troubleshooting process. •Although tools can be used in this step, a conversation with the user is often very helpful.
Step 2. Establish a Theory of Probable Causes	•After the problem is identified, try to establish a theory of probable causes. •This step often yields more than a few probable causes to the problem.
Step 3. Test the Theory to Determine Cause	•Based on the probable causes, test your theories to determine which one is the cause of the problem. •A technician may apply a quick fix to test and see if it solves the problem. •If a quick fix does not correct the problem, you might need to research the problem further to establish the exact cause.
Step 4. Establish a Plan of Action and Implement the Solution	After you have determined the exact cause of the problem, establish a plan of action to resolve the problem and implement the solution.
Step 5. Verify Solution and Implement Preventive Measures	•After you have corrected the problem, verify full functionality. •If applicable, implement preventive measures.
Step 6. Document Findings, Actions, and Outcomes	•In the final step of the troubleshooting process, document your findings, actions, and outcomes. •This is very important for future reference.

Resolve or Escalate?

- In some situations, it may not be possible to resolve the problem immediately. A problem should be escalated when it requires a **manager decision, some specific expertise, or network access level unavailable to the troubleshooting technician**.
- A company policy should clearly state when and how a technician should escalate a problem.

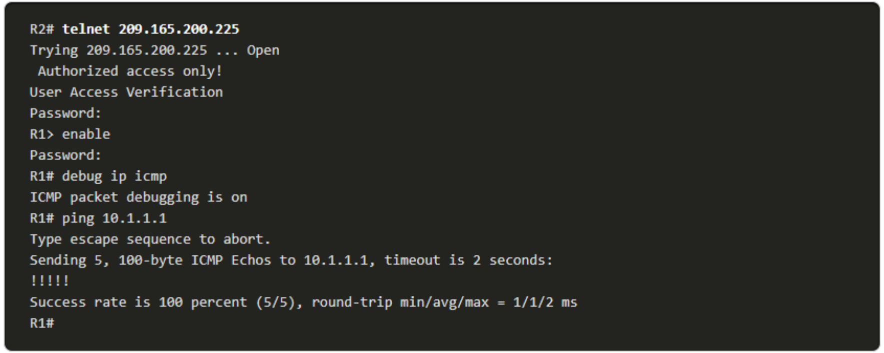
Troubleshooting Methodologies
The debug Command

- The IOS **debug** command allows the administrator to display OS process, protocol, mechanism and event messages in real-time for analysis.
- All **debug** commands are entered in privileged EXEC mode. The Cisco IOS allows for narrowing the output of **debug** to include only the relevant feature or subfeature. Use **debug** commands only to troubleshoot specific problems.
  - To list a brief description of all the debugging command options, use the **debug ?** command in privileged EXEC mode at the command line.
  - To turn off a specific debugging feature, add the **no** keyword in front of the **debug** command
  - Alternatively, you can enter the **undebug** form of the command in privileged EXEC mode.
  - To turn off all active debug commands at once, use the **undebug all** command.
- Be cautious using some **debug** commands, as they may generate a substantial amount of output and use a large portion of system resources. The router could get so busy displaying **debug** messages that it would not have enough processing power to perform its network functions, or even listen to commands to turn off debugging.

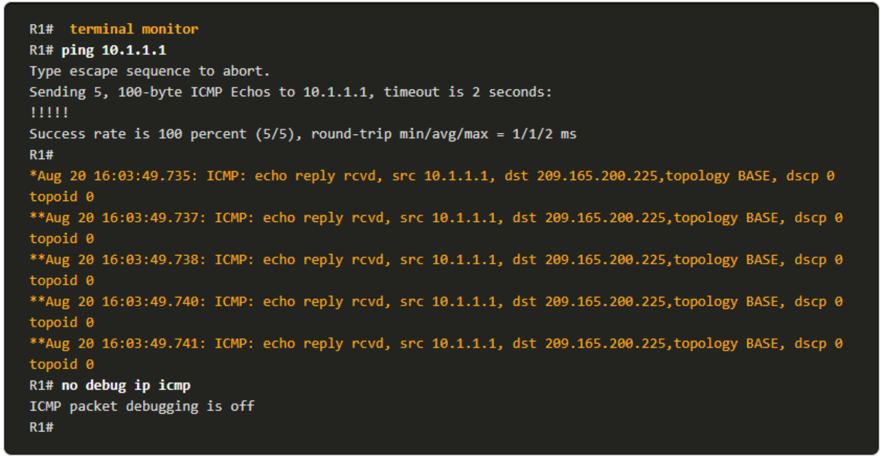
Troubleshooting Methodologies

The terminal monitor Command

- **debug** and certain other IOS message output is not automatically displayed on remote connections. This is because log messages are prevented from being displayed on vty lines.
- To display log messages on a terminal (virtual console), use the **terminal monitor** privileged EXEC command. To stop logging messages on a terminal, use the **terminal no monitor** privileged EXEC command.



```
R2# telnet 209.165.200.225
Trying 209.165.200.225 ... Open
 Authorized access only!
User Access Verification
Password:
R1> enable
Password:
R1# debug ip icmp
ICMP packet debugging is on
R1# ping 10.1.1.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.1.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/2 ms
R1#
```



```
R1#  terminal monitor
R1# ping 10.1.1.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.1.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/2 ms
R1#
*Aug 20 16:03:49.735: ICMP: echo reply rcvd, src 10.1.1.1, dst 209.165.200.225,topology BASE, dscp 0
topoid 0
**Aug 20 16:03:49.737: ICMP: echo reply rcvd, src 10.1.1.1, dst 209.165.200.225,topology BASE, dscp 0
topoid 0
**Aug 20 16:03:49.738: ICMP: echo reply rcvd, src 10.1.1.1, dst 209.165.200.225,topology BASE, dscp 0
topoid 0
**Aug 20 16:03:49.740: ICMP: echo reply rcvd, src 10.1.1.1, dst 209.165.200.225,topology BASE, dscp 0
topoid 0
**Aug 20 16:03:49.741: ICMP: echo reply rcvd, src 10.1.1.1, dst 209.165.200.225,topology BASE, dscp 0
topoid 0
R1# no debug ip icmp
ICMP packet debugging is off
R1#
```

17.8 Module Practice and Quiz

What Did I Learn In This Module?

- Factors to consider when selecting network devices for a small network are cost, speed and types of ports/interfaces, expandability, and OS features and services.
- When implementing a network, create an IP addressing scheme and use it on end devices, servers and peripherals, and intermediary devices.
- Redundancy can be accomplished by installing duplicate equipment, but it can also be accomplished by supplying duplicate network links for critical areas.
- The routers and switches in a small network should be configured to support real-time traffic, such as voice and video, in an appropriate manner relative to other data traffic.
- There are two forms of software programs or processes that provide access to the network: network applications and application layer services.
- To scale a network, several elements are required: network documentation, device inventory, budget, and traffic analysis.
- The ping command is the most effective way to quickly test Layer 3 connectivity between a source and destination IP address.
- The Cisco IOS offers an "extended" mode of the ping command which lets the user create special types of pings by adjusting parameters related to the command operation.

What Did I Learn In This Module (Cont.)?

- A trace returns a list of hops as a packet is routed through a network.
- There is also an extended traceroute command. It allows the administrator to adjust parameters related to the command operation.
- Network administrators view the IP addressing information (address, mask, router, and DNS) on a Windows host by issuing the ipconfig command. Other necessary commands are **ipconfig /all**, **ipconfig /release** and **ipconfig /renew**, and **ipconfig /displaydns**.
- Verifying IP settings by using the GUI on a Linux machine will differ depending on the Linux distribution (distro) and desktop interface. Necessary commands are ifconfig, and ip address.
- In the GUI of a Mac host, open Network Preferences > Advanced to get the IP addressing information. Other IP addressing commands for Mac are ifconfig, and networksetup -listallnetworkservices and networksetup -getinfo <network service>.
- The **arp** command is executed from the Windows, Linux, or Mac command prompt. The command lists all devices currently in the ARP cache of the host, which includes the IPv4 address, physical address, and the type of addressing (static/dynamic), for each device.
- The **arp -a** command displays the known IP address and MAC address binding.

What Did I Learn In This Module (Cont.)?

- Common show commands are **show running-config**, **show interfaces**, **show ip address**, **show arp**, **show ip route**, **show protocols**, and **show version**. The **show cdp neighbor** command provides the following information about each CDP neighbor device: identifiers, address list, port identifier, capabilities list, and platform.
- The **show cdp neighbors detail** command will help determine if one of the CDP neighbors has an IP configuration error.
- The **show ip interface brief** command output displays all interfaces on the router, the IP address assigned to each interface, if any, and the operational status of the interface.
- The six basic steps to troubleshooting Step 1. Identify the problem Step 2. Establish a theory of probably causes. Step 3. Test the theory to determine the cause. Step 4. Establish a plan of action and implement the solution. Step 5. Verify the solution and implement preventive measures. Step 6. Document findings, actions, and outcomes.
- A problem should be escalated when it requires a decision of a manager, some specific expertise, or network access level unavailable to the troubleshooting technician.
- OS processes, protocols, mechanisms and events generate messages to communicate their status. The IOS debug command allows the administrator to display these messages in real-time for analysis.
- To display log messages on a terminal (virtual console), use the terminal monitor privileged EXEC command.

Module 17: Build a Small Network

New Terms and Commands

- network applications
- application layer services
- extended ping
- extended traceroute
- network Baseline
- **ifconfig**
- **netsh interface ip delete arpcache**
- scientific method
- **debug**
- **terminal monitor**