75Dineshchandra / Google-IT-Support-Professional-Cert-Notes Public
forked from Clifton893/Google-IT-Support-Professional-Cert-Notes

Code Pull requests Actions Projects Wiki Security Insights Settings

main Google-IT-Support-Professional-Cert-Notes / Course-2 / c2-week-6.md Go to file ...

Clifton893 Update c2-week-6.md Latest commit 6c85d58 on Nov 28, 2020 History

1 contributor

304 lines (209 sloc) | 15.5 KB Raw Blame

Week 6: Troubleshooting and the Future of Networking

Intro

Protocols and devices feature built-in functionalities to help protect against issues. These functionalities are known as error detection and error recovery.

- **Error detection** is the ability for a protocol or program to determine that something went wrong.
- **Error recovery** is the ability for a protocol or program to attempt to fix it.

Verifying Connectivity

Ping: Internet Control Message Protocol

Internet Control Message Protocol (ICMP)

ICMP is mainly used by a router or remote host, to communicate why a transmission has failed, back to the origin of the transmission.

The makeup of an ICMP packet is a header and a data section:

- The first field is the **type field**, 8 bits long and specifying what type of message is being delivered.
  - Examples include `destination unreachable`, `time exceeded`, etc.
- Then comes the 8-bit **code field**, which indicates a more specific reason for the message than just the type.
  - Example: `destination network unreachable`, `destination port unreachable`, etc
- Next is a 16-bit checksum.
- Then the **rest of header** field, an optional 32-bit field.
  - Used to send more data by specific types and codes.
- Then the **data payload** for the ICMP packet.

The payload for an ICMP packet exists entirely so that the recipient of the message knows which of their transmissions caused the error being reported.

- It contains the entire IP header;
- And the first 8 bytes of the data payload section of the offending packet.

Ping

ICMP wasn't designed to be human-readable; it was intended for computers.

That's where ping comes into play.

- **Ping** lets you send a special type of ICMP message called an **Echo Request**.
  - If the destination is up and running and able to communicate on the network, it'll send back an ICMP **Echo Reply** message type.

Ping exists on basically every operating system.

- On Windows, Ping defaults to only four Echo requests.
- On MacOS and Linux, Ping will run forever until it's interrupted by the user inputs an interrupt event.
  - This is done with `^c`

Traceroute

Traceroute is a utility that lets you discover the path between two nodes, and gives you information about each hop along the way.

This covers connections at the network layer.

- Traceroute uses the TTL field, setting it to 1 for the first ICMP packet; then 2 for the second; and so on.
- On Linux and MacOS, trace route sends UDP packets to very high port numbers.
- On Windows--the command is `tracert` --defaults to the ICMP echo request.

There are two other, long-running tools similar to traceroute:

- `mtr` on Linux and MacOS
  - Works in real time, and will continually update its output with all the current aggregate dta about the traceroute;
- `pathping` on Windows
  - Runs for 50 seconds and then displays the final aggregate data all at once.

Testing Port Connectivity

There are two powerful tools to test connectivity at the transport layer:

- Netcat on Linux and MacOS,
- Test-NetConnection on Windows

Netcat

- The **Netcat** tool can be run through the command `nc` and has two mandatory arguments:
  i. A host;
  ii. And a port.
- If the connection succeeds, the blinking cursor will await more input.
  - This is a way to actually send application layer data to the listening service from your own keyboard.
- If you're only curious about the status of a report, you can issue the command with the `-z` flag
- Or you can use the `-v` flag to issue a Verbose command
  - This makes the command output useful to human eyes
    - (This is opposed to non-verbose output, which is best for usage in scripts.)
- By issuing a command with the -z and -v flags, the command's output will simply tell you if a connection to the port in question is possible or not.

Test-NetConnection

- If you run Test-NetConnection with only a host specified, it will default to using an ICMP echo request (much like ping)
  - But it displays way more data than a ping, including the data link layer protocol being used
- Issuing Test-NetConnection with the `-port` flag, you can ask it to test connectivity to a specific port

Digging into DNS

Name Resolution Tools

The most common command line tool for investigating domain name resolution is **nslookup**

- `nslookup` is available on MacOS, Linux, and Windows
- Execute the command with the host name following it:
  - The output displays what server was used to perform the request and resolution result.
- The tool also features an interactive mode, to search for additional options and run many more queries.
  - Enter interactive mode by running `nslookup` without any host name following it;
  - The angle bracket will act as your prompt
    - You can ask for A records, AAAA records, MX records, or even txt records associated with the host.
    - This is done by entering `set type=` followed by a resource record type.
    - Or enter `set debug` to display the full response packets (though this is a lot of data)

Public DNS Servers

An ISP almost always give you access to a recursive name server, as part of the server it provides.

Some Internet organizations run what are called public DNS servers.

- **Public DNS servers are name servers specifically set up so that anyone can use them, for free.
- Level 3 Communications has run arguably the most commonly-used public DNS servers
  - They range from `4.2.2.1` through `4.2.2.6`
- Google also operates public DNS servers
  - These are at `8.8.8.8` and `8.8.4.4`
- Most public DNS servers also respond to ICMP echo requests, so they're a good choice for testing general Internet connectivity using ping.

Always research before configuring any of your devices to public DNS servers, as crackers can easily hijack outbound DNS requests with faulty responses (which lead to malicious sites).

DNS Registration and Expiration

A **registrar** is an organization responsible for assigning individual domain names to other organizations or individuals.

Originally, there were few registrars, with the most notable being Network Solutions Inc.

The U.S. government and Network Solutions Inc. came to an agreement to let other companies also sell domain names.

Hosts Files

The original way that numbered network addresses were correlated with words, was through hosts files.

A **hosts file** is a flat file that contains, on each line, a network address followed by the host name it can be referred to as.

- For example, a line might read: 1.2.3.4 webserver
  - This means that oon the computer where this hosts file resides, a user could just refer to "webserver" instead of the IP address.
  - A user could just type "webserver" into a web browser's URL bar, or could issue a Ping webserver command and it would be translated to the IP address.

Hosts files are old, but all modern operating systems (including mobile) stil have hosts files

- This is because of a special IP address: The loopback address.
- A **loopback address** always points to itself, so a loopback address is a way of sending network traffic to yourself.
- Sending traffic to a loopback address bypasses all network infrastructure itself and traffic like that never leaves the node.

Almost every hosts file in existence will, in the very least, contain a line that reads `127.0.0.1 localhost`, most likely followed by `::1 localhost`, where ::1 is the loopback address for IPv6.

Also, hosts files are a popular way for computer viruses to disrupt and redirect users' traffic.

- Hosts files are examined before a DNS resolution attempt occurs on almost every major operating system
- This lets you force an individual computer to think a certain domain name always points to a specific IP

The Cloud

What is The Cloud?

The cloud isn't a single technology, or invention, or anything tangible at all.

Cloud computing is a technological approach where computing resources are provisioned in a shareable way, so that lots of users get what they need, when they need it.

Virtualization

- At the heart of cloud computing is a technology known as hardware virtualization
- Hardware virtualization is a core concept of how cloud computing technologies work
  - It allows the concept of a physical machine and a logical machine to be abstracted away from each other.
- With **virtualization**, a single physical machine, called a "host," could run many individual virtual instances, called "guests."
- Hardware virtualization platforms employ what's called a hypervisor.

A **hypervisor** is a piece of software that runs and manages virtual machines, while also offering these guests a virtual operating platform that's indistinguishable from actual hardware.

- Through virtualization, a single physical computer can act as the host for many independent virtual instances
- They each run on their own independent operating system and, in many ways, are indistinguishable from the same operating systems running on the physical hwrdware.
- The cloud takes this concept one step further.

Cloud Computing

A **public cloud** is a large cluster of machines run by another company.

A **private cloud** is used by a single large corporation, and generally physically hosted on its own premises.

A **hybrid cloud** is a term used to describe situations where companies might run things like their most sensitive proprietary technologies on a private cloud; while entrusting their less-sensitive servers to a public cloud.

In summary, cloud computing is a new model in computing where large clusters of machines let us use the total resources available in a better way.

Everything as a Service

Anothe rterm used more and more with the rise of cloud computing is *X as a service*, where X stands for many different things.

Infrastructure as a Service (IaaS)

- The idea behind IaaS is you shouldn't have to worry about building your own network, or your own servers.
- You just pay someone else to provide you with that service.

Platform as a Service

- A subset of cloud computing, where a platform is provided for customers to run their services
- This basically means that an execution engine is provided for whatever software someone wants to run

Software as a Service

- While IaaS abstracts away the physical infrastructure you need; and PaaS abstracts the server instances you need;
- SaaS is essentially a way of licensing the use of software to others while keeping that software centrally-hosted and managed
  - An example would be email, such as Gmail (by Google) or Office 365 Outlook (by Microsoft)

More and more, the point of a business's network is just to provide an Internet connection to access different software or data in the cloud.

Cloud Storage

In a **cloud storage system**, a customer contracts a cloud storage provider to keep their data secure, accessible, and available.

- Abstract away managing a storage array, and hardware issues
- Available across many geographic regions
  - This provides protection against data loss
- Grows with you, managing your expenses for what you actually need

IPv6

IPv6 Addressing and Subnetting

- The biggest difference between IPv4 and IPv6 is the number of bits reserved for an address.
  - IPv4 addresses are 32 bits; so there can be around 4.2 billion individual addresses;
  - IPv6 addresses are 128 bits in size; this is an unfathomable, 39 digit-long number.
- IPv6 addresses are usually written out as 8 groups of 16-bits each.
  - These groups are further made up of four hexadecimal numbers.
- But the full IPv6 address is still way too long and unwieldy, so there is a notation that breaks them down even more:

There are two rules for shortening an IPv6 address:

1. You can remove any leading zeroes from a group.
2. Any number of consecutive groups composed of just zeroes can be replaced with two colons.

- This can only happen once, for any specific address
- Otherwise, you couldn't know exactly how many zeroes were replaced by the double colons.

The IPv6 loopback address is thirty-one 0s with a 1 at the end; which can be condensed to `::1`.

Reserved Spaces

- `2001:0db8` is reserved for documentation and education
- `FF00::` is reserved for multicast
  - **Multicast** is a way of addressing groups of hosts all at once
- `FE80::` are used for link-local unicast
  - **Link-local unicast addresses** allow for local network segment communications and are configured based upon a host's MAC address
    - Used by an IPv6 host to receive their network configuration (much like how DHCP works)
    - The host's MAC address is run through an algorithm to turn it from a 48-bit number into a unique 64-bit number;
    - Then it's inserted into the address's host ID.

Address Classes

These don't exist in IPv6, since the vast address space doesn't need them.

The first 64-bits of any IPv6 address is the network ID; and the second 64-bits of any IPv6 address is the host ID.

Subnetting

- IPv6 uses the same CIDR notation as IPv4.
- This is used to define a subnet mask against the network ID portion of an IPv6 address.

IPv6 Headers

One of the more elegant improvements of IPv6 was in its header:

- The first field is the **version field**
  - A 4-bit field that defines what version of IP is in use
- The next field is the **traffic class** field
  - This is an 8-bit field that defines the type of traffic contained within the IP datagram, and allows for different classes of traffic to receive different priorities.
- Next is the **flow label field**
  - A 20-bit field that's used in conjunction with the traffic class field, for routers to make decisions about the quality of service level for a specific datagram.
- Next is the **payload length field**
  - A 16-bit field that defines how long the data payload section of the datagram is
- Then the **next header field**
  - A unique concept to IPv6
  - The IPv6 header was built to be as short as possible; this was accomplished by abstracting away many of the optional header fields from IPv4
  - The **next header field** allows to chain together different header fields, if there is a lot of optional configuration.
- Next is the **hop limit field**
  - An 8-bit field that's identical in purpose to the TTL field in an IPv4 header
- Finally come the **source address** and **destination address** fields
  - These are each 128 bits
- If the next header field specified another header, it would follow at this time.
- If not, a data payload (the same length as specified in the payload length field) would follow.

IPv6 and IPv4 Harmony

The IPv6 specs have set aside a number of addresses that can be directly correlated to an IPv4 address.

- Any IPv6 address that begins with 80 zeroes, and is then followed by 16 ones, is understood to be part of the IPv4 mapped address space
- The remaining 32 bits of the IPv6 address is just the same 32 bits of the IPv4 address it's meant to represent.

IPv6, during its adoption, will need a way to travel over the old IPv4 remnants of the Internet backbone.

- This is being achieved with **IPv6 tunnels**
- They consist of IPv6 tunnel servers, on each side of a connection.
- **IPv6 tunnel** servers take incoming IPv6 traffic and encapsulate it within traditional IPv4 datagrams.
- This is then delivered across the IPv4 Internet space, where it's received by another IPv6 tunnel server
- That server de-encapsulates the datagram and passes the IPv6 traffic further along the network.

IPv6 tunnel broker

These are companies that provide IPv6 tunneling endpoints for you, so you don't have to introduce additional equipment to your network.

Questions for review

Keywords

Concepts