Contents

Index

Index

7 Steps of The “Network Troubleshooting Methodology”

- Troubleshoot network cockups with these 7 easy to follow steps:
    1. Identify the problem
    2. Establish a theory of probable cause
    3. Test the theory to determine the cause
    4. Establish a plan of action to resolve the problem and identify potential effects
    5. Implement the solution or escalate as necessary
    6. Verify full system functionality and if applicable implement preventative measures, and
    7. Document findings, actions, outcomes, and lessons learned.

6 Steps of the CompTIA Troubleshooting Methodology

- For the exam, it is important that you can list and identify these steps in order:
    1. Identify the problem.
    2. Establish a theory of probable cause (question the obvious).
    3. Test the theory to determine the cause.
    4. Establish a plan of action to resolve the problem and then implement the solution.
    5. Verify full system functionality and, if applicable, implement preventative measures.
    6. Document findings, actions, and outcomes.

7-Step Malware Removal Process

1. Investigate and verify malware symptoms
2. Quarantine the infected systems
3. Disable System Restore in Windows
4. Remediate the infected systems, update anti-malware software, scan the system, and use removal techniques (e.g., safe mode, pre-installation environment)
5. Schedule scans and run updates
6. Enable System Restore and create a restore point in Windows, and
7. Educate the end user.

If this were a home user's machine, the above would be an appropriate response, but you should follow the company's procedures if it were a corporate workstation. Most companies require any machines suspected of malware infection to be scanned/analyzed by the cybersecurity department before remediating or reimaging them. Therefore, the best thing to do would be to inform the cybersec department after steps 1 & 2 above.

Index

The CIA Triad of Cybersecurity: Confidentiality, Integrity & Availability

The CIA Triad is a security model that helps people think about various parts of IT security:

- ✓ Confidentiality is concerned with unauthorized people seeing the contents of the data
- ✓ Integrity ensures that no unauthorized modifications are made to the information
- ✓ Availability is concerned with the data being accessible when and where it is needed

Keep In Mind!

- Whether a questions asks for the "BEST" or "FIRST" solution to an issue!

- Compatibility in the answer-options to the questions: sometimes the details within the options are incompatible! For example, for a network connectivity issues the options may state, "the SFP on the workstation is malfunctioning", but SFPs are not installed on workstations, they're installed on network devices such as switches etc so the option is easily dismissed. In another case, the option may be, "APIPA is incorrectly configured on the switch", however APIPA is a Windows feature and is configured on the workstation, not elsewhere!

Index

Hardware - Networking

Tools

Loopback Plug is used to test a port: it involves connecting pin 1 to pin 3 and pin 2 to pin 6.

- You can do this either by rewiring the jack or twisting the relevant pairs together on a cable stub. Alternatively, you can purchase a prefabricated loopback plug.
- When you connect a loopback plug to a port, you should see a solid connection LED.
- You can also use the loopback plug in conjunction with diagnostic software.

Crimper is a tool used to attach an RJ-45 plastic connector to an unshielded twisted pair (UTP) or shielded twisted pair (STP) cable.

- It pushes a portion of the plastic into the jacket of the cable to hold it in place.

Cable Tester is used to ensure a cable is properly created as a patch cable (straight through) or a crossover cable.

- Cable testers provide detailed information on the physical and electrical properties of the cable.
- For example, they test & report cable conditions, crosstalk, attenuation, noise, resistance, and other cable run characteristics.

Punchdown Tools are used to connect an ethernet cable to the back of a patch panel, a punchdown block, or the back of a network wall jack.

Tone Generator & Probe: A tone generator is connected to a wall jack and sends a repeating signal over the cable. The probe can then be used to detect which cable is attached to the wall jack by detecting the signal being sent by the tone generator.

- The probe needs to be near or touch the cable with the tone generator attached to identify it positively.
- While a multimeter could be used (in resistance mode) to determine if two ends of a cable are attached to the same cable, the distance between the user's office and the communication closet would prevent a multimeter from being used in most cases.

Time-Domain Reflectometer is used to determine exactly where in a network cable a break has occurred. Once the location is identified, the cable can be repaired or spliced to return it to normal operations.

An Optical Time Domain Reflectometer (OTDR) is used by organizations to certify the performance of new fiber optics links and detect problems with existing fiber links. An OTDR can identify if a fiber cable is broken and provide an approximate location for the break in meters or feet.

Cable Snip/Cable Cutter is used to cut copper cables into shorter lengths from a longer spool of wound cable.

Cable Stripper is a hand-held tool that is used to remove the insulation or outer sheath from copper cables such as UTP, STP, or coaxial cables.

Index

Fusion Splicer is used to create long fiber optic cable lengths by splicing multiple cables together or to repair a break in a fiber optic cable.

A (Fiber) Light Meter, also known as an **optical power meter**, is used to **measure the power** in an optical signal over a fiber optic cable. A fiber light meter could be used to test if the cable is broken, but it would not be able to determine where the break in the fiber cable is located

A Media Converter is a layer 1 networking device that connects two different media types, such as a copper twisted pair cable and a fiber optic cable.

Q: You are troubleshooting a cable modem for a home user's network. The connection speeds are much lower than you expected. You suspect the coaxial cable between the wall jack and the cable modem is faulty. Based on your research, a coaxial cable used in data networks should have an impedance of 50 ohms. Which of the following tools should you use to measure the resistance of the coaxial cable?

A: Multimeter

Notice: The use of the term "impedance" is a classic case of confusing wording used in CompTIA exam questions: Both 'impedance' and 'resistance' describe the same concept: the resistance or hinderance of a medium to conduct electricity, i.e. the flow of electrons in a medium. While resistance is more commonly used for this, sometimes it can technically be used to describe the resistance of a resistor, while impedance is the term employed to quantify the same hinderance effect caused by electrical components such as inductors & capacitors in a circuit.

Q: When installing a network cable with multiple strands, a network technician pulled the cable past a sharp edge. This resulted in the copper conductors on several of the wire strands being exposed. If these exposed conductors come into contact with each other, they can form an electrical connection. Which of the following conditions would result in this scenario?

A: Short

Q: Your company has just gotten a new OC-12 installed to support your datacenter. The telecommunications provider has installed the connection from their main offices to your demarcation point. You connect the OC-12 to your network, but you are noticing many dropped packets and errors. You suspect this may be a layer 1 issue. Which of the following tools can you use to help identify the source of the issue on this connection?

A: Use an OTDR to validate the integrity of the cable

You may not know all the details involved in this question, but that is ok. Start with what you do know. The question talks about an OC-12 connection, which is an optical carrier or fiber optic cable. Based on that, you know the only one of these options has anything to do with a fiber cable, and that is the OTDR (Optical Time-Domain Reflectometer). An optical time-domain reflectometer (OTDR) is an optoelectronic instrument used to characterize an optical fiber. An OTDR injects a series of optical pulses into the fiber under test and extracts, from the same end of the fiber, light that is scattered (Rayleigh backscatter) or reflected back from points along the fiber. The other three options can only be used with copper cables, like UTP, STP, and coaxial cables.

Index

Networking Devices

Routers can connect LANs to WANs, something that should have been obvious given that's the device you've installed at home to access the global internet.

- A router is a network device that links dissimilar networks and can support multiple alternate paths between locations based upon the parameters of speed, traffic loads, and cost.
- Routers are used to logically divide networks into subnets.
- A router or other gateway device must be installed between two VLANs to allow connections to be routed between them.
- Each switchport on a router is a separate collision domain and a **separate broadcast domain**.
- A router operates at the network layer (Layer 3) of the OSI model and makes routing decisions based upon IP addresses.

Hub provides no intelligence in its interconnection functions so that whatever is received on one port is repeated out every other port, thus all devices connected to a hub are **within a single collision domain and a single broadcast domain, therefore they must use half-duplex for communications and CSMA/CD**. This leads to many collisions occurring on the hub and increases the number of rebroadcasts which slows down the entire network. As a result, hubs are no longer used and are considered legacy devices. Hubs, Repeaters & Wireless Access Points (WAPs) operate at the physical layer (Layer 1).

Switch is a network device that receives incoming data into a buffer, then the destination MAC address is compared with an address table so that data is only sent out to the port with the corresponding MAC address. In a switched network, each port is in a separate collision domain. A switch operates at OSI Layer 2 (Datalink). **VLANS are configured on network switches!** Port Mirroring is used on a network switch to send a copy of network packets seen on one switch port to a network monitoring connection on another switch port.

A Multilayer Switch combines the features of a switch and a router into a single device. **For the exam, unless they mention a "multilayer / layer 3 switch", always assume they are referencing a basic layer 2 switch.**

Managed Switch is a switch with advanced networking functions and security settings that can be enabled and configured by an administrator. These switches also separate broadcast domains.

Hubs and switches may also act as signal repeaters, resetting the effective length of cables transiting through them. For example, an 80meter CAT cable coming into a switch/hub will have its length reset to 0mts so only the distance from the switch/hub to any follow-on networking devices/end-points would matter, thus extending the 100mts CAT length-limit. Hubs, however, will also introduce errors on the network as all connected devices will be placed into a single collision & broadcast domain, so they're not preferable. Also, while repeaters may be used for this, a switch might be the better choice depending on the scenario.

A Network Bridge is a computer networking device that creates a single, aggregate network from multiple communication networks or network segments. This function is called network bridging. **Bridging is distinct from routing**: Routing allows multiple networks to communicate independently and yet remain separate, whereas bridging connects two separate networks **as if they were a single network. In the OSI model, bridging is performed in the data link layer (layer 2).** If one or more segments of the bridged network are wireless, the device is known as a **wireless bridge**.

Index

Optical Network Terminal (ONT) is a device that connects **fiber optics cables to other types of wiring** such as Ethernet and phone lines by converting the signal from optical to electrical and vice versa. An ONT is commonly used with fiber to the house (FTTH) installations.

Cable Modems Cable providers will install devices called 'Cable Modems' to get internet into your house via a coax cable. **It looks like a router but isn't!** There'll be a separate router installed too.

A cable modem is a type of network bridge that provides bi-directional data communication via radio frequency channels on a hybrid fiber-coaxial (HFC), radio frequency over glass (RFoG), & coaxial cable infrastructure. Cable modems are primarily used to deliver broadband internet access as cable internet, taking advantage of the high bandwidth of HFC and RFoG networks.

Satellite Systems provide far greater coverage area than can be achieved using other technologies. A Very Small Aperture Terminal (VSAT) Microwave Antenna is aligned to an orbital satellite that can either relay signals between sites directly or via another satellite.

Microwave Links require a direct line of sight (LoS) between the antennas to maintain a strong and effective link. These line-of-sight microwave links use highly directional transmitter and receiver antennas to communicate via a narrowly focused radio beam. **WiMAX** is a type of microwave connection.

Q: Your co-worker has just installed an unmanaged 24-port switch. He is concerned with the amount of broadcast traffic that may exist when using this device. How many broadcast domains are created when using this single 24-port switch?

A:1

A single 24-port unmanaged switch will have only 1 broadcast domain. Routers and VLANs split up broadcast domains. Since this is an unmanaged switch, it will only have a single broadcast domain, but it will have 24 collision domains. If this was a managed layer 3 switch, it could provide routing functions and break apart the broadcast domains. But, since this was an unmanaged switch, there must be only 1 broadcast domain on this switch.

Q: A technician is called to investigate a connectivity issue to a remote office connected by a fiber optic cable. Using a light meter it is determined that there is excessive dB loss. The installation has been working for several years. The switch was recently moved to the other side of the room and a new patch cable was installed. Which of the following is most likely the reason for the excessive dB loss?

A: Dirty connectors

When fiber optic connectors become dirty, signal loss can cause severe problems and performance issues. Something as simple as oil from a technician's hand can render a fiber connector dirty and cause a loss of signal. The technician will need to use appropriate cleaning cloth to clean the dirty connectors and restore the service.

Since the switch was only moved to the other side of the room, it is unlikely that it now exceeds the distance limitations for a fiber cable since those are measured in hundreds of meters.

The question does not mention that the cable was bent or moved around a corner, therefore it is unlikely to be a bend radius limitation affecting the signal.

Index

Fiber optic cables use different wavelengths depending on the type of fiber optic cable being used. Multimode fibers use 850 or 1300 nanometer wavelengths, whereas single-mode fibers use 1550 nanometer wavelengths. It is unlikely that the wrong patch cable was used as most organizations only implement a single type of fiber infrastructure to minimize the number and type of cables needed to support them.

Q: A network technician is troubleshooting connectivity problems between switches but suspects the ports are not properly labeled. What option will help to identify the switches connected to each port quickly?

A: Enable a discovery protocol on the network devices

By enabling a discovery protocol on the network devices, the technician will be able to get detailed information such as the IP addresses, system version, and device information from supporting devices directly. There are three primary discovery protocols: Simple Network Management Protocol (SNMP), Link Layer Discovery Protocol (LLDP), and ping.

Q: A user was moved from one cubicle in the office to a new one a few desks over. Now, they are reporting that their VoIP phone is randomly rebooting. When the network technician takes the VoIP phone and reconnects it in the old cubicle, it works without any issues. Which of the following is MOST likely the cause of the connectivity issue?

A: Cable Short

Since the scenario states the VoIP phone works properly from the old desk, it is properly configured and the hardware itself works. This indicates the problem must be caused by the new desk which contains a different network cable from the switch to the wall jack in the cubicle. This is most likely a bad cable, such as one with a short in it. To verify this theory, the technician should use a cable tester to verify if the cable does have a short or not. While attenuation is a possible cause of the problem described, it is unlikely since the employee only moved a few desks (10-15 feet), and is not a large enough distance to cause significant attenuation issues.

Q: Students at Dion Training are working on a networking lab that requires a single switch to be remotely accessed by many students simultaneously. The instructor verifies that the switch can be accessed using the console, but the switch is only letting one student log in to the device at a time. Which of the following configurations should the instructor implement to fix this issue?

A: Increase the number of virtual terminal available

You can set a limit of how many virtual terminals can simultaneously remotely connect to a switch. The issue in this scenario is that the switch is configured to a maximum of one virtual terminal, so only one student can access the switch at a time. When a student connects to a switch or router using ssh or telnet, it requires a virtual terminal connection. The default virtual terminal limit is 32 on Cisco devices, but you can configure it to allow between 1 and 64 simultaneous connections. To connect to a virtual terminal, you would utilize a terminal emulator. A packet capture tool is used to collect data packets being transmitted on a network and save them to a packet capture file (pcap) for later analysis.

Index

Q: A network technician receives the following alert from a network device: "High utilization threshold exceeded on gi1/0/24: current value 88%" What is being monitored to trigger the alarm?

A: Port Utilization

The message has been triggered on the interface link status since gi1/0 is a gigabit interface.

Q: You are investigating a network connectivity issue that is affecting two of your network clients. When you check the switchports of these clients, you observe that the switchports' physical interfaces are continually going up and down. Which of the following is the most likely reason for the flapping of the switchports you are observing?

A: Duplicate MAC address

One indication of this occurring is when a switch continually changes the port assignments for that address as it updates its content-addressable memory (CAM) table to reflect the physical address and switchport bindings. This will cause the switchports to continually flap by going up and down as the assignments are updated within the CAM table. Multicast flooding occurs because no specific host is associated with the multicast MAC address in the content-addressable memory (CAM) table of a switch.

Index

Collision Domains

Q: You are installing a Small Office/Home Office (SOHO) network consisting of a router with 2 ports, a switch with 8 ports, and a hub with 4 ports. The router has one port connected to a cable modem and one port connected to switch port #1. The other 6 ports on the switch each have a desktop computer connected to them. The hub's first port is connected to switch port #2. Based on the description provided, how many collision domains exist in this network?

A: 9

Based on the description provided, there are 9 collision domains. Each port on the router is a collision domain (2), each port on the switch is a collision domain (8), and all of the ports on the hub make up a single collision domain (1). But:

- ***since one of the ports on the router is connected to one of the switch ports, they are in the same collision domain (-1).***
- ***Similarly, the hub and the switch share a common collision domain connected over the switch port (-1).***

This gives us 9 collision domains total: the 8 ports on the switch and the 1 port on the route that is used by the cable modem

Q: A small law office has a network with three switches (8 ports), one hub (4 ports), and one router (2 ports). Switch 1 (switch port 8) is connected to an interface port (FastEthernet0/0) on the router. Switch 2 (switch port 8) and switch 3 (switch port 8) are connected to Switch 1 (switch ports 1 and 2). The hub has three computers plugged into it on ports 1, 2, and 3. The fourth port on the hub is connected to the router's other interface port (FastEthernet0/1). Based on the configuration described here, how many collision domains are there within this network?

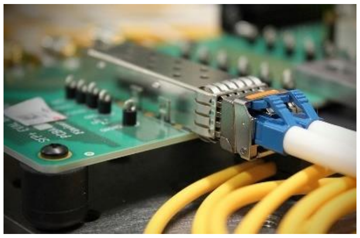
A: 4

A collision domain is a network segment connected by a shared medium or through repeaters where simultaneous data transmissions collide with one another. Hubs do not break up collision domains, but routers and switches do. For each switchport or interface on a switch or router, there is a new collision domain. Therefore, in this network, you will have one collision domain for the hub and its clients that are connected to FastEthernet0/1. There is a second collision domain for the router's other interface (FastEthernet0/0) that is shared with Switch 1 (switch port 8). There is a third collision domain for the connection between Switch 2 and Switch 1, and a fourth domain for the connection between Switch 3 and Switch 1. If there were additional clients on any of these switches, each client would also be a part of its own collision domain, but since none were mentioned, we only have 4 collision domains in this network.

Index

Small Form-Factor Pluggable (SFP) Transceiver

A small form-factor pluggable (SFP) transceiver is a compact, hot-swappable, input/output transceiver used in data communication and telecommunications networks. SFP interfaces **between communication devices like switches, routers (NOT workstations!)** and fiber optic cables, and performs conversions between optical and electrical signals.



Antennas

A Patch Antenna is a type of radio antenna with a low profile, which can be mounted on a flat surface. A patch antenna is typically mounted to a wall or a mast and provides coverage in a limited angle pattern. Patch antennas can be directional or omnidirectional, but a directional antenna should be used for a connection between two buildings within line of sight of each other.

A Yagi or Directional Antenna could also be used, but if the distance is smaller than about 300 feet between the buildings, a patch antenna would be sufficient. A Yagi would be utilized for longer distances instead, but these do weigh more and have a larger footprint. Think of a meditating Yogi: focused and directed in his meditation on some far-off land.

A Whip Antenna is a vertical omnidirectional antenna that is usually utilized in indoor environments. A whip antenna is omnidirectional and cannot be used for directional use cases. Think of the “cantenna” antenna made from Pringles cans, and of whipped-cream dip for the ultimate chips & dip!

Omni-Directional Antennas broadcast radio frequencies in all directions creating a large sphere of coverage. The antenna has the capability to send and receive signals in a circumference around the antenna.

Directional Antennas broadcast radio frequencies in a single direction (unidirectional) or two directions (bidirectional) to create a zone or area of coverage.

High-Gain Antennas put out increase signal strengths and can reach further distances with fewer wireless access points (WAPs) than low gain antennas.

Low-Gain Antennas spread the power out across a wider volume in space, but the signal reaching the receivers is weaker and harder to process.

Index

Wi-Fi Generations

Generation	IEEE Standard	Maximum Linkrate (Mbit/s)	Adopted	Radio Frequency (GHz)
Wi-Fi 7	802.11be	1376 to 46120	(2024)	2.4/5/6
Wi-Fi 6E	802.11ax	574 to 9608	2020	6
Wi-Fi 6			2019	2.4/5
Wi-Fi 5	802.11ac	433 to 6933 (theoretical 3.5 Gbps as per the exam!)	2014	5
Wi-Fi 4	802.11n	72 to 600	2008	2.4/5
*(Wi-Fi 3)**	802.11g	6 to 54	2003	2.4
*(Wi-Fi 2)**	802.11a	6 to 54	1999	5
*(Wi-Fi 1)**	802.11b	1 to 11	1999	2.4
*(Wi-Fi 0)**	802.11	1 to 2	1997	2.4

One way 802.11n and 802.11ac networks achieve superior throughput and speeds by using multiple-input multiple-output (MIMO) and multi-user MIMO (MU-MIMO), respectively. MIMO uses multiple antennas for transmission and reception, which results in higher speeds than 802.11a and 802.11g networks.

Wireless N and Wireless AC networks also utilize the 5 GHz frequency band, allowing them to achieve speeds greater than 54 Mbps, and AC uses Orthogonal Frequency-Division Multiple Access (OFDMA) to conduct multiplexing of the frequencies transmitted to and received at each client to provide additional bandwidth.

WPA2 is a wireless encryption standard and can be used with Wireless G, N, AC, or AX.

LightWeight Access-Point Protocol (LWAPP) is the name of a protocol that can control multiple Wi-Fi Wireless Access Points (WAPs) at once. This can reduce the amount of time spent on configuring, monitoring, or troubleshooting a large network. LWAPP does not affect the speed of a wireless network.

Received Signal Strength Indication (RSSI)

The Received Signal Strength Indication (RSSI) is an estimated measure of the power level that a radio frequency client device receives from a WAP. If the RSSI is -90dB to -100dB, it indicates an extremely weak connection and insufficient wireless coverage in the area where the device is operating.

REMEMBER THAT A HIGH SIGNAL-TO-NOISE (SNR) RATIO IS A GOOD THING!

Index

Wi-Fi Bands and Channels

- The Wi-Fi frequency band for **2.4 GHz** is split into **14 channels of 5 MHz each**.

  -> United States and Canada, only channels 1 through 11 may be used.

  -> Europe, channels 1 through 13 may be used.

  -> Japan, channels 1 through 14 may be used.
- With WAPs that run 2.4 GHz frequencies, you can only select channels between 1 and 11 in the United States. This includes 802.11b, 802.11g, 802.11n, and 802.11ax networks.

  To Prevent Overlapping of the Channels, you should select channels 1, 6, and 11. By doing so, you can increase the reliability and throughput of your wireless network.
  - Since each Wi-Fi communication requires approximately 20 MHz to operate effectively, users should set their WAPs to channels 1, 6 & 11 to minimize interference & avoid overlapping channels.
- **The 5 GHz spectrum provides 24 non-overlapping channels**
- **2.4GHz Wi-Fi only supports 3 non-overlapping channels (1, 6, 11)**

Q: Which of the following wireless characteristic does channel bonding improve?
A: Connection Speed

BSSID & ESSID

With an ESSID (Extended Service Set), a wireless network can utilize multiple wireless access points to broadcast a single network name for access by the clients.

A BSSID (Basic Service Set) can only utilize a single access point in each wireless network.

Access Point (AP) Isolation

Access Point (AP) isolation is a technique for preventing mobile devices connected to an AP from communicating directly with each other.

Q: A network administrator is tasked with building a wireless network in a new building located next door to your company's office building. The wireless clients should not be able to communicate with other wireless clients but should be able to communicate with any wired users on the network. The users must be able to seamlessly migrate between the buildings while maintaining a constant connection to the LAN. How should the administrator configure the new wireless network in this new building?

A: Use the same SSID on different channels and AP Isolation: For users to be able to seamlessly migrate between the two buildings, both APs must use the same SSIDs. To prevent frequency interference, though, each device needs to select a different and non-overlapping channel to utilize. Finally, the AP isolation should be enabled.

Index

Cable Details – Types & Ranges

Coaxial Cable used to transmit video, communications, and audio. Most commonly used for cable TV service.

- Coaxial cables are a specialized type of copper cabling that uses a copper core to carry the electrical signal while being enclosed by plastic insulation and shielding to protect the data transmission from the effects of electromagnetic interference (EMI).
- Both RG-6 and RG-59 are cable types used for coaxial cable connections. RG-6 cabling is recommended for your Cable TV, satellite, TV antennas, or broadband internet and uses the **F-Type connector**. RG-59 cabling is generally better for most CCTV systems and other analog video signals.
- Coaxial Cables can cover a maximum distance of 200 to 500 meters in length.

Plenum-rated Cable has a special insulation that has low smoke and low flame characteristics.

- Plenum cable is mandated to be installed in any air handling space.

Shielded Cables contain a braided foil shield around the inner cabling to protect the data from the effects of electromagnetic interference (EMI). STP (Shielded Twisted Pair) is a type of cabling that can help prevent electrical interferences or cross-talk.

- Cross-talk is when electrical interference can cause CRC (Cyclic Redundancy Check) Errors.
- A CRC is used to calculate checksums before and after data transfers to ensure accuracy.
- If electrical interference gets in the way, such as proximity to fluorescent light bulbs, it can cause data to be corrupted and produce an error.

Shielded & Plenum Copper Cables can only cover a distance of approximately 100 meters in length.

Optical Fiber Cables consists of an ultra-fine core of glass to carry the light signals surrounded by glass or plastic cladding, which guides the light pulses along the core, and a protective coating.

- The fiber optic cable is contained in a protective jacket and terminated by a connector.
- Fiber optic cables use light signals to carry data across a cable at extremely high bandwidths.

Serial Cable is a data cable that transmits data a single bit at a time. A DB-9 connector is used to terminate an RS-232 serial cable.

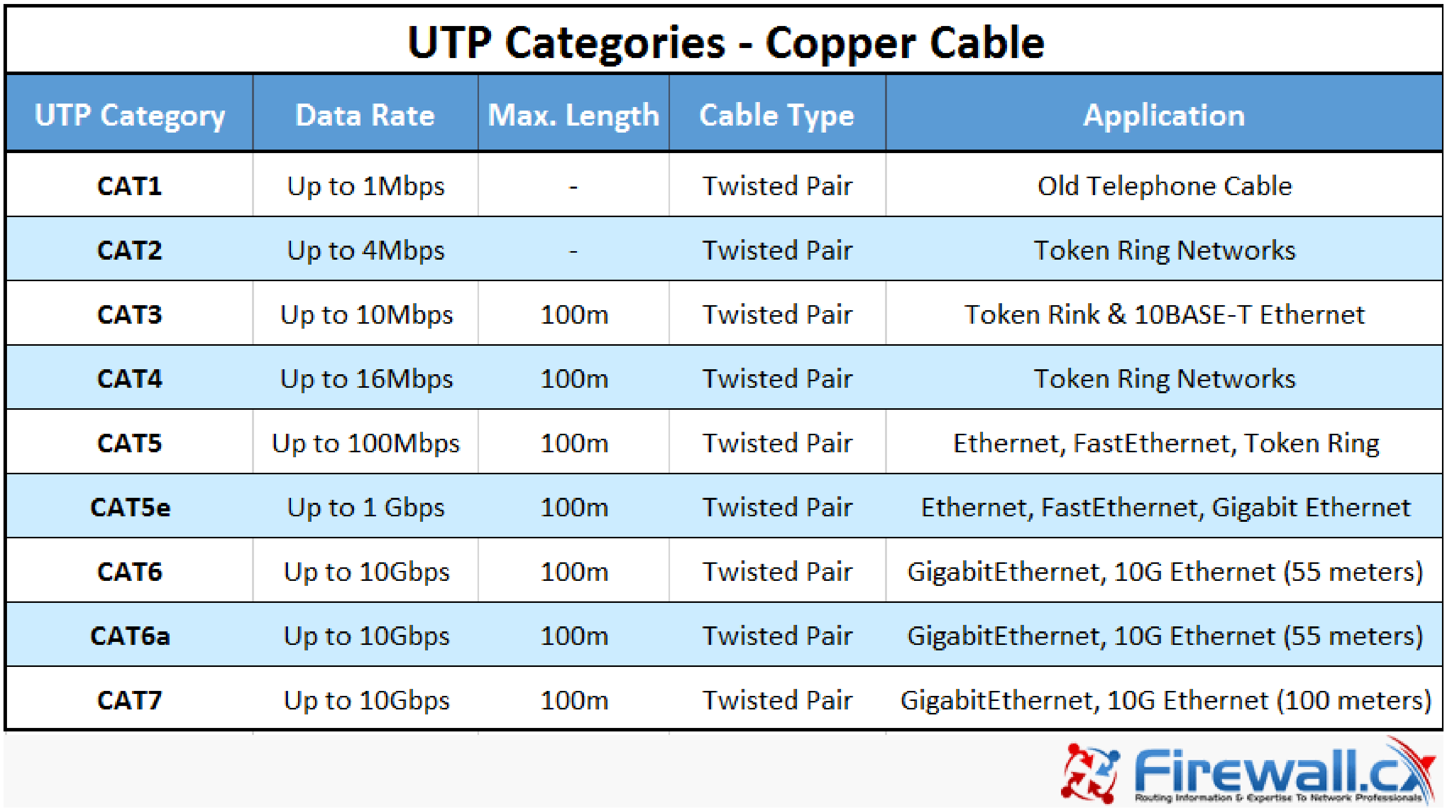
Rollover or Console Cables are used to connect a computer to a **console port** on a router for configuration.

Twinaxial cabling, or "Twinax", is a type of cable similar to coaxial cable, but with two inner conductors instead of one. Due to cost efficiency, it is commonly used in very short-range high-speed differential signaling applications, such as SATA 3.0 cables and uplinks between SFP+ modules in switches or routers.

Fiber Optic Cables are network cables that contains strands of glass fibers inside an insulated casing. They're designed for long-distance, high-performance data and telecommunications. If you are dealing with connecting two networks over a long distance (over a few hundred meters), you should use a fiber optic cable.

Index

CAT Talk



UTP Categories - Copper Cable

UTP Category	Data Rate	Max. Length	Cable Type	Application
CAT1	Up to 1Mbps	-	Twisted Pair	Old Telephone Cable
CAT2	Up to 4Mbps	-	Twisted Pair	Token Ring Networks
CAT3	Up to 10Mbps	100m	Twisted Pair	Token Rink & 10BASE-T Ethernet
CAT4	Up to 16Mbps	100m	Twisted Pair	Token Ring Networks
CAT5	Up to 100Mbps	100m	Twisted Pair	Ethernet, FastEthernet, Token Ring
CAT5e	Up to 1 Gbps	100m	Twisted Pair	Ethernet, FastEthernet, Gigabit Ethernet
CAT6	Up to 10Gbps	100m	Twisted Pair	GigabitEthernet, 10G Ethernet (55 meters)
CAT6a	Up to 10Gbps	100m	Twisted Pair	GigabitEthernet, 10G Ethernet (55 meters)
CAT7	Up to 10Gbps	100m	Twisted Pair	GigabitEthernet, 10G Ethernet (100 meters)

CAT6 can do 1Gbps – 100m and 10Gbps – 55m. CAT6a can do 10Gbps – 100m. CAT7 came before CAT6a and can use a TERA connector instead of just the RJ45.

CAT: Power over Ethernet (PoE), PoE+, and VoIP – 802.3af & 802.3at

- VoIP (Voice over IP) devices that rely on PoE (Power over Ethernet) should use a **CAT 5e, CAT 6, or higher cable** to make the connection. This allows a single cable (CAT 5e or CAT 6) to carry both the data and the device's power. POE is defined in the IEEE 802.3af.
  - Fiber, coaxial, and CAT 3 cables cannot carry power to the VOIP device and cannot be used to meet this requirement.
  - Using a CAT 5e or CAT 6 cable, you can connect two devices of approximately 300 feet (100 meters) without any need to repeat the signal.
  - The 802.3af (PoE) standard can support up to 15.4W of power at up to 100m distance.
  - The 802.3at (PoE+) standard can support up to 25W of power at up to 100m distance.
  - PoE+ can support higher-powered devices such as PTZ cameras, door controllers, & thin clients
- To prevent VoIP calls from being dropped,
  Quality of Service (QoS) should be implemented on the switch: QoS means using a network protocol to prioritize certain traffic types over others
  - Enterprise networks can use QoS protocols to make sure traffic such as Voice over IP calling or video conferencing is given higher priority than traffic where packet-timing is less important, such as ordinary file downloads.

MTU (Maximum Transmission Unit) is the largest unit that can be transmitted across a network. If the MTU is set at a value above 1500, the network is configured to support jumbo frames.

Placing VoIP devices on a separate VLAN is performance optimization!

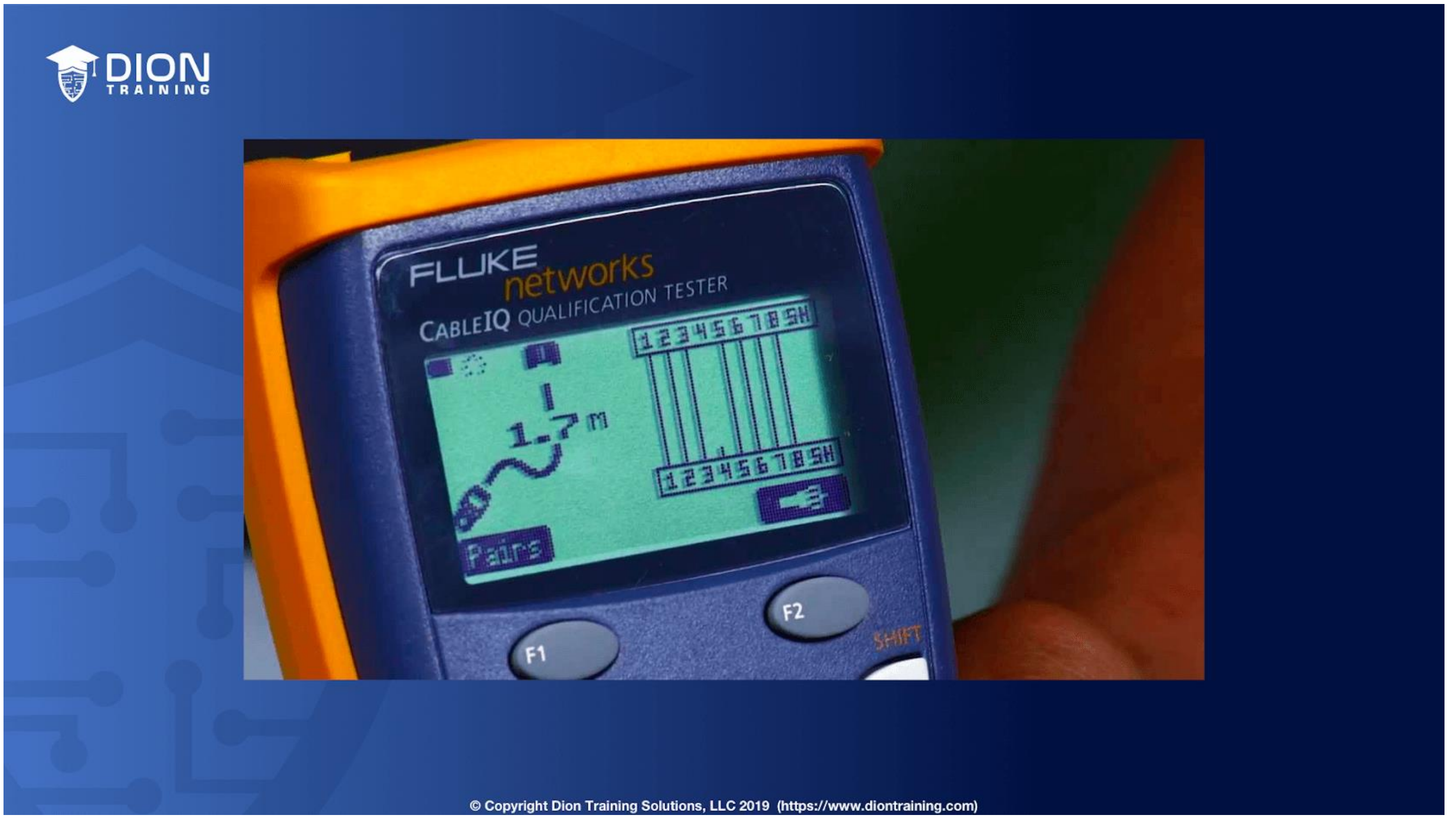
Index

Crossover Cables and Straight-Through/Patch Cables (STPC)

Crossover Cables should be used to connect two similar devices (**PC to PC, Router to Router, Switch to Switch**, etc.) to create a network. For an ethernet cable, this should be a network cable with a T568A wiring standard on one end and a T568B wiring standard on the other end of the cable to create a crossover cable.

Straight-Through / Patch Cable is a network cable that uses the same wiring standard on both ends such as T568A to T568A or T568B to T568B and is used to connect complimentary devices, **such as PCs to routers**. **Remember this by thinking that you bought an ethernet cable on Amazon straight away without checking the type!**

Q: Based on the output of the cable tester below, what kind of ethernet cable is this?

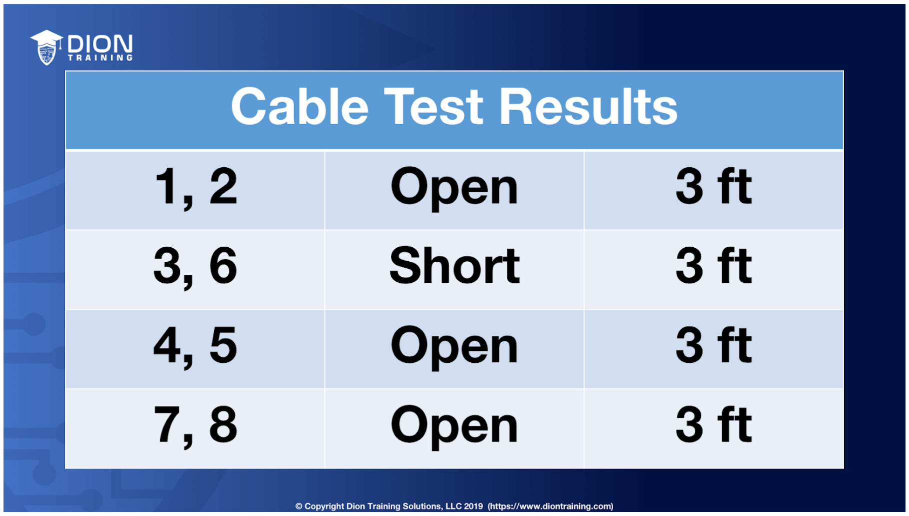


A: Straight-Through / Patch Cable

This is a patch cable (also known as a straight-through cable), as indicated by the matching of the Tx and Rx pins (pins 1, 2, 3, and 6) on both sides of the cable. Additionally, you may have noticed that there is an open on this cable on pin 4 since it is not sending a signal from pin 4 to pin 4 in the diagram. A crossover cable would have pins crossing from one side to the other, such as pin 1 going to pin 6. A rollover cable has opposite pin assignments on each end of the cable, such as pin 1 going to pin 8, pin 2 going to pin 7, etc. An RG-6 cable only has one internal copper wire, not 8 as shown in this diagram for a twisted-pair copper cable.

Index

Q: Using the results provided from a cable certifier, was the cable properly crimped or not?



Cable Test Results		
1, 2	Open	3 ft
3, 6	Short	3 ft
4, 5	Open	3 ft
7, 8	Open	3 ft

A: Nope

Cable certifiers can provide a “pass” or “fail” status following the industry standards and can also show detailed information such as “open,” “short,” or the length of the cable. When a short is detected, but the cable's full length is shown (3 ft), this indicates the cable was incorrectly crimped. In this case, it appears that pin 3 and pin 6 are both crimped into the same position in the RJ-45 connector, causing the short. An open indicates that the electrical signal is not reaching the other end of the cable. Both of these are indications of an incorrectly crimped cable.

Q: When installing a network cable with multiple strands, a network technician pulled the cable past a sharp edge. This resulted in the copper conductors on several of the wire strands being exposed. If these exposed conductors come into contact with each other, they can form an electrical connection. Which of the following conditions would result in this scenario?

A: Short (NOT ‘crosstalk’!)

A short is an electrical term that is an abbreviation for a short circuit. A short generally means that an unintended connection between two points is allowing current to flow where it should not. In this scenario, the short is caused by the damaged cable in which two or more of the conductors are connected. This has caused the cable to fail and will report as "short" when using a cable tester.

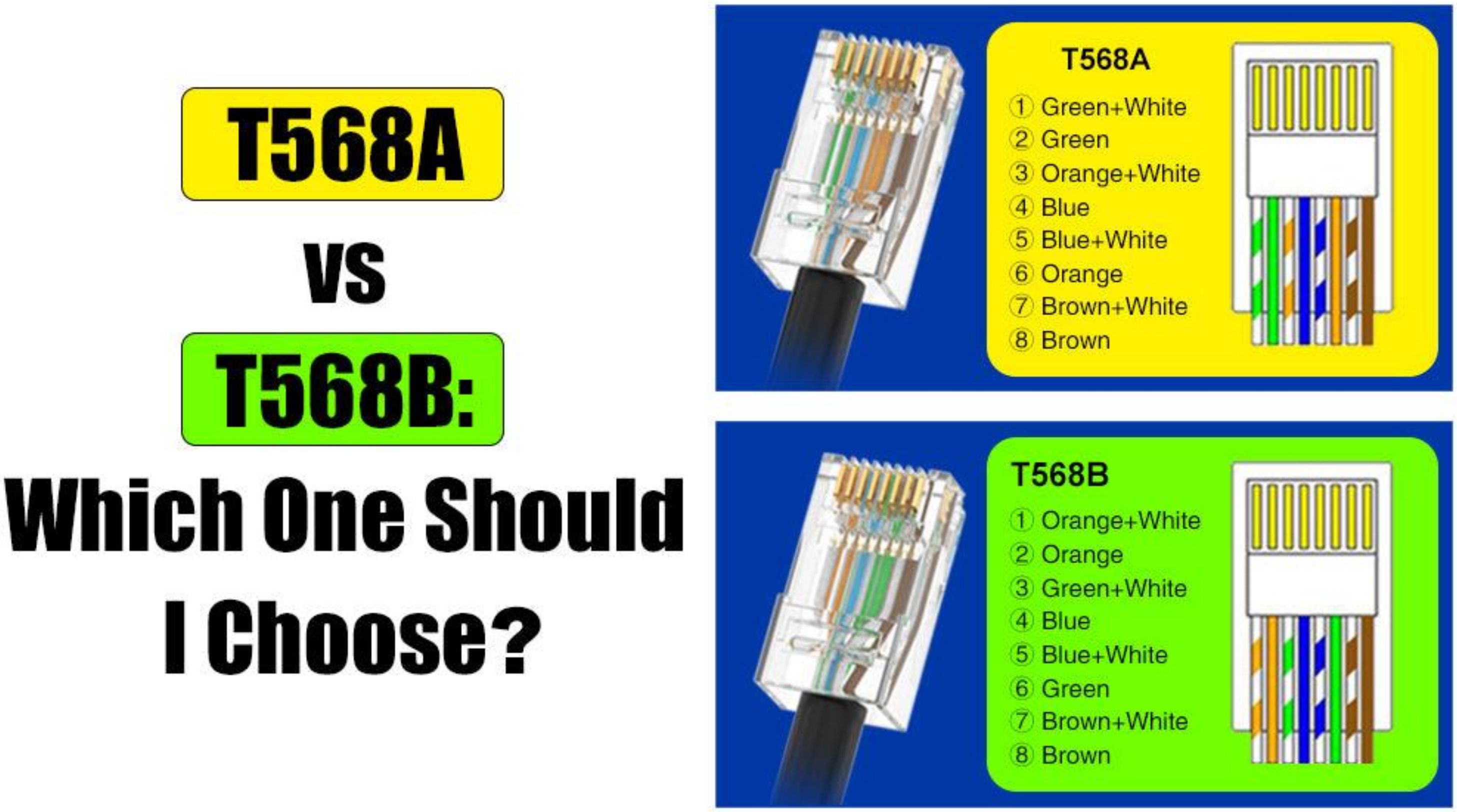
An open is reported when there is no connection between the two ends of a cable or wire. This can occur when a wire or cable is accidentally cut in half. An open is the opposite of a short.

Electrostatic discharge is the sudden flow of electricity between two electrically charged objects.

Crosstalk is the coupling of voltage to an adjacent line through mutual coupling composed of a mutual inductance, a coupling capacitance, or both. Crosstalk occurs within a twisted pair cable when the pairs become untwisted, or no shielding or insulation remains.

Index

T-568A & T-568B Connector Colors



Q: (This is a simulated Performance-Based Question.) What is the correct color scheme for Pin 1 to Pin 8 for a T-568A connector?

A: white/green, green, orange/white, blue, white/blue, orange, white/brown, brown

<u>You need to have the T-568-A and T-568-B standards memorized before test day because you may be asked to perform a drag and drop exercise of placing the right colored wires into the right numbered pins based on a T-568A or T-568B connector. Remember, a straight-through cable will have T-568B on both ends. If you are asked to make a cross-over cable, you need a T-568A on one side and a T-568B on the other side.</u>

<u>STUDY TIP:</u>

1. First, notice that in both connectors, the central of the 8-wires on pin 4 & 5 are the same: blue, with the solid blue wire first
2. Next, notice that for all other wires, the solid color is *after* the white+color wire!
3. Now, for the B cable, remember, "**O**h **G**ee, it's **B**!" for OGB: Orange, Green and Brown!
4. Since B is easy to remember now, for A just remember the funny-sounding word "GOB"!

Index

Legacy Switches and MDIX

Q: Max is a network technician who just terminated the ends on a new copper cable used between two legacy switches. When he connects the two switches using the cable, they fail to establish a connection. What is MOST likely the issue?

A: The cable is a straight-through cable

There are two types of cable, Straight-through and Crossover. In this instance, a crossover cable would need to be used to communicate with legacy switches since they won't support MDIX. A Medium Dependent Interface Crossover (MDIX) is a version of the Medium Dependent Interface (MDI) enabling a connection between corresponding devices, such as a switch to another switch. If the switch doesn't MDIX, then you must use a crossover cable to connect them.

Bend radius cannot be the correct answer to this question since copper cables are being used and not fiber cables. Bend radius is a concern when using fiber cables as it leads to increase reflections and a decrease in signal strength.

An RJ-11 connector only has 6 pins and is smaller than an RJ-45 connector. The technician would visually be able to see the difference as the RJ-11 connector would not fit properly in the switchports. (this despite the exam’s claims to question the obvious first!)

Q: A technician is troubleshooting a workstation at Dion Training. The workstation is suffering from intermittent connectivity issues. The technician notices that the STP cable pairs are not completely twisted near the connector. Which of the following issues may be experienced because of this?

A: Crosstalk

Crosstalk is defined as an effect caused by the unintentional and undesired transmission (leakage) of a signal from one cable to another. Crosstalk can occur if the twisted pairs are not twisted sufficiently, because the twisting of the cable pairs reduces crosstalk between neighboring cable pairs. The twisting is done to help cancel exterior electromagnetic interference. To solve this cable's crosstalk issue, the cable pairs should be trimmed down and the cable re-terminated again properly.

The EIA/TIA-568A and EIA/TIA-568B wiring standards utilize different colored cable pairs on each end of a cable. If you use a mismatch of the two standards on the same cable, it will create a cable that cannot be used as a straight-through or patch cable. This would not lead to intermittent connectivity, though, it would lead to a scenario with no connectivity.

A split pair error occurs when one wire from each of two different pairs gets swapped identically on both ends of the cable. The result is a cable that will pass a standard continuity test, but will have serious cross-talk problems, and will most likely not perform adequately at specified data rates. Split pairs were commonly used in older Cat 3 copper networks, but are no longer used in Cat 5 or above networks. The scenario in this question describes a crosstalk issue, not a split pair issue, though.

Index

Fiber

<u>Connectors:</u> A ST, SC, LC, or MTRJ connector is used to terminate a fiber optic cable.

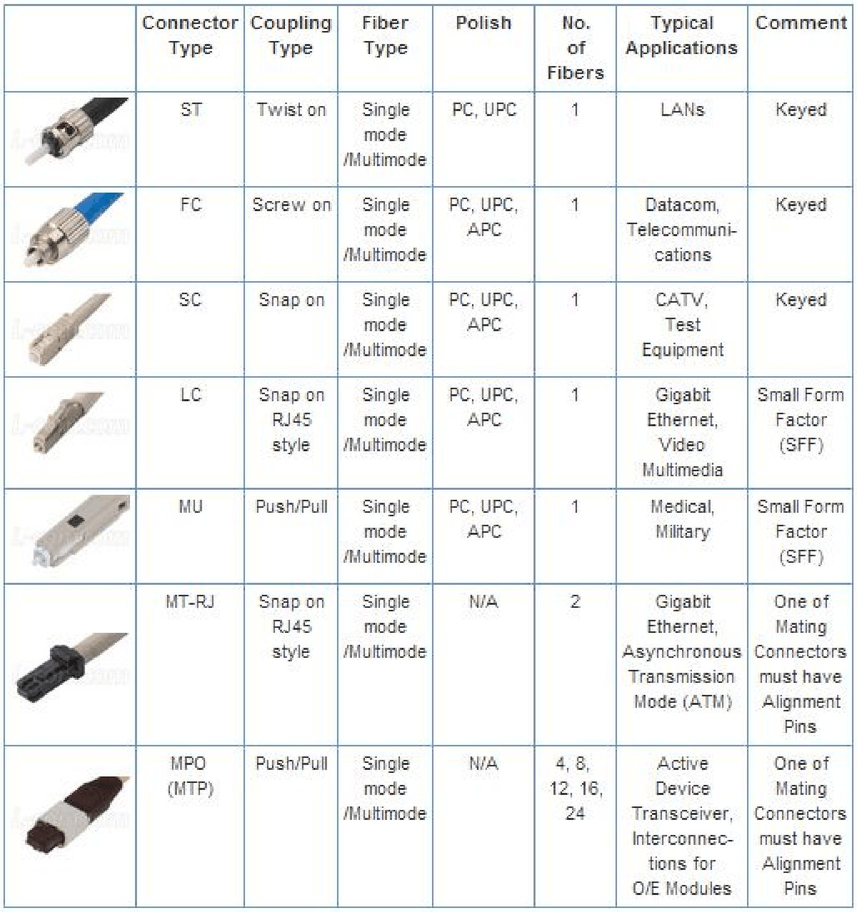
<u>ST (Straight Tip) Connector i</u>s a quick-release bayonet-style connector that has a long cylindrical connector. **Commonly used in LAN networking applications.**

<u>SC (Subscriber/Standard Connector)</u> is a general-purpose push/pull style connector that has a square, snap-in connector that latches with a simple push-pull motion.

- SC connectors are widely used in single-mode fiber optic systems.

<u>LC (Lucent Connector)</u> is a small form factor connector that combines the transmit and receive cables into a single square, snap-in connector. These can be single duplex or use two connectors for double duplex.

<u>F-Type Connector</u> is used with coaxial cables, not fiber optic cables.



	Connector Type	Coupling Type	Fiber Type	Polish	No. of Fibers	Typical Applications	Comment
	ST	Twist on	Single mode /Multimode	PC, UPC	1	LANs	Keyed
	FC	Screw on	Single mode /Multimode	PC, UPC, APC	1	Datacom, Telecommunications	Keyed
	SC	Snap on	Single mode /Multimode	PC, UPC, APC	1	CATV, Test Equipment	Keyed
	LC	Snap on RJ45 style	Single mode /Multimode	PC, UPC, APC	1	Gigabit Ethernet, Video Multimedia	Small Form Factor (SFF)
	MU	Push/Pull	Single mode /Multimode	PC, UPC, APC	1	Medical, Military	Small Form Factor (SFF)
	MT-RJ	Snap on RJ45 style	Single mode /Multimode	N/A	2	Gigabit Ethernet, Asynchronous Transmission Mode (ATM)	One of Mating Connectors must have Alignment Pins
	MPO (MTP)	Push/Pull	Single mode /Multimode	N/A	4, 8, 12, 16, 24	Active Device Transceiver, Interconnections for O/E Modules	One of Mating Connectors must have Alignment Pins

<u>MTRJ</u> is commonly used to connect fiber optic cables **to a switch or router**, but it uses a single connector that houses the Tx and Rx connections.

<u>"Fiber to the X" (FTTx)</u> is commonly used to describe where the fiber connection ends between the service and the subscriber. The closer the fiber is to the user's network, the faster the service:

<u>FTTH (Fiber to the House)</u> provides fiber directly to the user's home network making it the fastest option. Traditionally, you will find a 1 Gbps connection or higher with FTTH.

<u>FTTN (Fiber to the Node) or FTTC (Fiber to the Curb/Cabinet) </u>provides fiber only to the local area or neighborhood but then uses copper cabling from the node/cabinet/curb to the home network, which slows down the network (generally, 100-200 Mbps).

<u>HFC (Hybrid Fiber Coax)</u> is similar to FTTN/FTTC, except that coaxial cable is used from the cabinet to the home to increase the speed (generally 300-500 Mbps).

<u>OC-3 & OC-12 (Optical Connector)</u> is a type of fiber connection.

The <u>transmit (Tx) & receive (Rx)</u> reversed is a common issue with fiber optic patch cables.

Index

Q: Which communication technology would MOST likely be used to increase bandwidth over an existing fiber-optic network by combining multiple signals at different wavelengths?

A: DWDM

Dense Wavelength-Division Multiplexing (DWDM) is a high-speed optical network type commonly used in MANs (metropolitan area networks). DWDM uses as many as 32 light wavelengths on a single fiber, where each wavelength can support as many as 160 simultaneous connections.

Q: A network technician has configured a point-to-point interface on a router. Once the fiber optic cables have been run, though, the interface will not come up. The technician has cleaned the fiber connectors and used a fiber light meter to confirm that light passes in both directions without excessive loss. Which of the following is MOST likely the cause of this issue?

A: There is a wavelength mismatch

Wavelength mismatch occurs when two different transceivers are used at each end of the cable. For example, if one SFP (Small Form-factor Pluggable transceiver) uses a 1310nm transceiver and the other end uses an 850 nm transceiver, they will be unable to communicate properly, and the link will remain down. Cross-talk and EMI do not affect fiber optic cables. The bend radius is how sharply a cable can safely bend without causing damage by creating micro cracks on the glass fibers.

Q: A network technician works with a junior technician when the network technician is called away for a more urgent issue. The junior technician orders an SC 80/125 fiber cable instead of an ST 80/125. Which of the following will MOST likely be an issue with the new cable?

A: Connector mismatch

Fibre Channel & FCoE

Fibre Channel (FC) is a high-speed data transfer protocol providing in-order, lossless delivery of raw block data. Fibre Channel is primarily used to connect computer data storage to servers in storage area networks (SAN) in commercial data centers. Fibre Channel typically runs on optical fiber cables within and between data centers, but can also run on copper cabling.

When the technology was originally devised, it ran over optical fiber cables only and, as such, was called "Fiber Channel". Later, the ability to run over copper cabling was added to the specification. In order to avoid confusion and to create a unique name, the industry decided to change the spelling and use the British English fibre for the name of the standard.

Fibre Channel over Ethernet (FCoE) is a computer network technology that encapsulates Fibre Channel frames over Ethernet networks. FCoE is commonly used in storage area networks internally to an organization's enterprise network. In other words, FCoE is a method of supporting converged Fibre Channel (FC) and Ethernet traffic on a Data Center Bridging (DCB) network.

Index

All Your 'Bases' Are Belong To Us!

Nomenclature: The "100" in the media type designation refers to the transmission speed of 100 Mbit/s, while the "BASE" refers to baseband signaling. The letter following the dash ("T" or "F") refers to the physical medium that carries the signal (twisted pair or fiber, respectively), while the last character ("X", "4", etc.) refers to the line code method used, where "X" is a placeholder for the FX and TX variants.

In telecommunication, a line code is a pattern of voltage, current, or photons used to represent digital data transmitted down a communication channel or written to a storage medium. Common line encodings are unipolar, polar, bipolar, and Manchester code.

- 10GBase-SR is a 10-Gigabit Short-Range (SR) Ethernet LAN standard for use with **Multimode-Fiber (MMF)** optic cables using short-wavelength signaling
- 10GBase-LR is a Long-Range (LR) standard for 10 Gigabit Ethernet over single-mode fiber optic cabling
- 1000Base-T and 40GBase-T are standards for Gigabit Ethernet over copper wiring
- 1000Base-FX and 1000Base-LR are standard for Gigabit Ethernet over single-mode fiber optic cabling
- 100BaseTX represents Fast Ethernet

For the exam, remember the memory aid, "S is NOT single," which means that if the naming convention contains Base-S as part of its name then it uses a multimode fiber cable.

Q: You have been asked to install a media converter that connects a newly installed multimode cable to the existing Cat 5e infrastructure. Which type of media converter should you use?

A: Fiber to Ethernet

Q: After upgrading a fiber link from 1 Gbps to 10 Gbps. A network technician ran a test of the link and the link is not connecting properly. The two routers are 450 meters apart and are connected using a MMF fiber with 10GBaseLR SFP+ transceivers. The fiber runs through the electrical and boiler rooms of each building. Which of the following is the MOST likely cause of the connectivity issues?

A: The wrong transceivers are being used

The transceivers being used are 10GBaseLR, which are used with single mode fiber (SMF), not multimode fiber (MMF). Since the network is already using MMF fiber and was previously working, the technician should replace the 10GBaseLR SFP+ transceivers with 10GBaseSR SFP+ transceivers instead.

Index

Cable, DSL, DOCSIS, T1 & POTS

Digital Subscriber Line (DSL) is a technology used to transmit multimedia traffic at high-bit rates **over twisted-pair copper wire (over ordinary telephone lines, also called "POTS" – Plain Old Telephone System!).** This allows the telecoms company to connect a user's home to the local switching center using normal telephone lines, then connect that local switching center (using a DSLAM (DSL Access Multiplexer) to multiplex the connections) to the central office over a single high-speed cable (such as a fiber connection).

POTS (Plain Old Telephone System) is an older standard used for telephone systems. An RJ-11 wiring standard is used to terminate both ends of a standard phone line. This is also used for DSL lines and VoIP ATA (Analog Telephony Adapter) devices.

An Analog Modem is a device that converts the computer's digital pulses to tones that can be carried over analog telephone lines and vice versa. DSL is the other type of Internet connection that uses an RJ-11 connection to a phone line.

A DOCSIS (Data Over Cable Service Interface Specifications) Modem is a cable modem and would require a coaxial cable with an F-type connector. DOCSIS is an international telecommunications standard that permits the addition of high-bandwidth data transfer to an existing cable television (CATV) system. It's used by many cable television operators to provide Internet access over existing Hybrid Fiber-Coaxial (HFC) infrastructure.

A T1 Line is a twisted copper wire that transfers voice and data from one location to another via digital signals. These lines have been the industry standard for decades thanks to their capacity. A T1 line can transmit the equivalent of 24 traditional voice channels, making it optimal for commercial buildings and **provides a guaranteed 1.544 Mbps of throughput.**

The T-carrier is a member of a series of carrier systems developed by AT&T Bell Laboratories for digital transmission of multiplexed telephone calls. It's a hardware specification for carrying multiple **Time-Division Multiplexed (TDM) telecommunications channels** over a single four-wire transmission circuit. It was developed by AT&T at Bell Laboratories ca. 1957 and first employed by 1962 for long-haul **Pulse-Code Modulation (PCM)** digital voice transmission with the D1 channel bank. The T-carriers are commonly used for trunking between switching centers in a telephone network, including to **Private Branch Exchange (PBX)** interconnect points. **It uses the same twisted pair copper wire that analog trunks used, employing one pair for transmitting, and another pair for receiving.** Signal repeaters may be used for extended distances.

The first version, the Transmission System 1 (T1), was introduced in 1962 in the Bell System, and could transmit up to 24 telephone calls simultaneously over a single transmission line of copper wire. Subsequent specifications carried multiples of the basic T1 (1.544 Mbit/s) data rates, such as T2 (6.312 Mbit/s) with 96 channels, T3 (44.736 Mbit/s) with 672 channels, and others.

Though the AT&T T-carrier system defines five levels, only T1 and T3 are commonly in use.

A Leased Line is a private telecommunications circuit between two or more locations provided according to a commercial contract, normally over a **fiber-optic connection**.

Q: Which type of internet connection is terminated at a local switching center and requires a different media type between the switching center and the end customer?

A: DSL

Index

Q: Which type of internet connection allows for high-speed bi-directional data communication over a hybrid fiber-coaxial (HFC) connection?

A: Cable (See 'coax'? Say Cable!)

Q: Which of the following WAN technologies would MOST likely be used to connect several remote branches that have no fiber, microwave, or satellite connections available?

A: POTS

Q: You have just moved into a new apartment and need to get internet service installed. Your landlord has stated that you cannot drill any holes to install new cables into the apartment. Luckily, your apartment already has cable TV installed. Which of the following technologies should you utilize to get your internet installed in your apartment?

A: DOCSIS modem

Q: You have been asked to select the best WAN connection for a new network at Dion Training. The company has stated that they must have a guaranteed throughput rate on their Internet connection at all times. Based on this requirement, what type of WAN connection should you recommend?

A: T-1

Dial-up, DSL, and cable broadband do not provide a guaranteed throughput rate. Instead, these services provide a variable throughput rate based on network conditions and demand in the area of your business.

Index

Modulation

Modulation is the process of varying one or more properties of a periodic waveform, called the carrier signal, with a separate signal called the modulation signal that typically contains the information to be transmitted. Wi-Fi can use different digital modulation schemes for data transmission. Common types of modulation include **Orthogonal Frequency-Division Multiplexing (OFDM), Quadrature Amplitude Modulation (QAM), and Quadrature Phase-Shift Keying (PSK)**

Time-Division Multiplexing (and PRI ISDN, PRI T-1, PSTN, CSMA/CD)

Time-division multiplexing allows for two or more signals or bitstreams to be transferred in what appears to be simultaneous sub-channels within one communication channel but is actually physically taking turns on the channel. This is the technology used in a single PRI ISDN or PRI T-1. (PRI: Primary Rate Interface; ISDN: Integrated Services Digital Network) service to essentially share a single cable but pass multiple voice calls over it. **PRI is thus a component of ISDN. ISDN uses point-to-point connections.**

Analog circuit switching is used by telephone providers on the Public Switched Telephone Network (PSTN), not with ISDN or T-1 connections. CSMA/CD is the Carrier Sense Multiple Access Collision Detection that is used for ethernet access at layer 2 of the OSI model. **CSMA/CD is not used with ISDN or T-1 connections.**

Time-division spread spectrum is not a real thing: spread spectrum is used in Wi-Fi but it is based on frequency, not time.

Q: Which of the following technologies deliver multiple voice calls over a copper wire if you have an ISDN or T-1 connection?

A: Time-Division Multiplexing

Q: You are troubleshooting your company's T-1 connection to your ISP. The ISP has asked you to place a loopback on the device which connects your T-1 line to their central office. Which of the following devices should you connect a loopback adapter to test the connection?

A: Channel Service Unit / Data Service Unit

A CSU/DSU (Channel Service Unit/Data Service Unit) is a hardware device about the size of an external modem that converts digital data frames from the communications technology used on a local area network (LAN) into frames appropriate to a wide-area network (WAN) and vice versa. A CSU/DSU is used to terminate a T1 connection at the customer's site.

Q: Your company wants to develop a voice solution to provide 23 simultaneous connections using VoIP. Which of the following technologies could BEST provide this capability?

A: T1

A T1 can transmit 24 telephone calls at a time because it uses a digital carrier signal (DS-1). DS-1 is a communications protocol for multiplexing the bit streams of up to 24 telephone calls simultaneously. The T1's maximum data transmission rate is 1.544 Mbps.

Index

Q: You have been asked to troubleshoot Dion Training's T1 connection that is experiencing connectivity issues. You have already verified that the network's router is properly configured, the cable is connected properly between the router and the T1's CSU/DSU, but the T1 remains down. You want to test the interface on the CSU/DSU to ensure it is functioning properly. Which of the following tools should you use to test this interface?

A: Loopback Adapter (NOT a cable tester!)

A T1 connection is a copper-based connection. A loopback adapter is a plug that is used to test the physical port or interface on a network device. You will need to insert the loopback adapter into the interface on the CSU/DSU and conduct a self-test of the device by looping back the transmit path to the receive path and the receive path to the transmit path. A loopback adapter can also be used to test the T1 line by allowing the ISP to conduct a remote diagnosis of the connection between their central office and your demarcation point to ensure it is working properly.

Unified Communications

Unified Communications (UC) enables people to use different modes of communication, media, and devices to communicate with anyone, anywhere, anytime. **To accomplish this, a UC gateway is needed.** Unified communications (UC) refers to the integration of multiple forms of real-time communications including voice, video, collaboration, and text messaging. A UC gateway connects your IP-based voice system to the Public Switched Telephone Network (PSTN).

Index

Patch Panels

A patch panel is a device or unit featuring a number of jacks, usually of the same or similar type, for the use of connecting & routing circuits for monitoring, interconnecting & testing circuits in a convenient, flexible manner. Patch panels are commonly used in computer networking, recording studios & radio & television.

A patch panel is used in a structured cabling system. For example, a computer is connected to a wall jack which is in-turn connected to a patch panel via cabling running through the walls. The pre-wired RJ-45 port on the patch panel is then connected to the network switch using a straight-through/patch cable.

Punchdown Blocks: 110 Blocks and Krone Blocks

A punch-down block (also punchdown block, punch block, punchblock, quick-connect block and other variations) is a type of electrical connection often used in telephony. **It is named because the solid copper wires are "punched down" into short open-ended slots which are a type of insulation-displacement connector.** These slots, usually cut crosswise (not lengthwise) across an insulating plastic bar, contain two sharp metal blades which cut through the wire's insulation as it is punched down.

A 110-PunchBlock

A 110 block is a type of punch-down block used to terminate runs of on-premises wiring in a structured cabling system. The designation 110 is also used to describe a type of insulation displacement contact (IDC) connector used to terminate twisted pair cables, which uses a punch-down tool similar to the type used for the older 66 block. **A 110 punchdown block provides more spacing between the terminals & is designed for Cat 5 networks to eliminate crosstalk between the cables**.

Krone LSA-PLUS (or simply krone) is an insulation-displacement connector for telecommunications. It is a proprietary European alternative to 110 block.

Index

Distribution Frames: MDFs and IDFs

If you work in a relatively large environment, you're going to work with a distribution frame. This is where there's passive cable termination, so this is not a powered system: you're instead terminating cables using a punch down block or a patch panel. These are usually located in the back of the data center or across a very large wall because you need a lot of real estate to be able to punch down that many different cable connections, so you often use this as the name of a room or a location.

And this may not be just for copper: you might also have fiber connections. There may be voice, video & data all combined on the same punch down block in the distribution frame. This is thus a very significant part of the network as you have all of the data for all of your systems passing through the distribution frame. In fact, if you want to find the MDF, you're probably also going to have to find the data center at the same time!

The central point of the network is usually the Main Distribution Frame (MDF). This is usually in your data center and is where you're terminating all your network connections, including WAN connections. If you need to go from the inside to the outside, you're going through the MDF! That means it's a good test point as well.

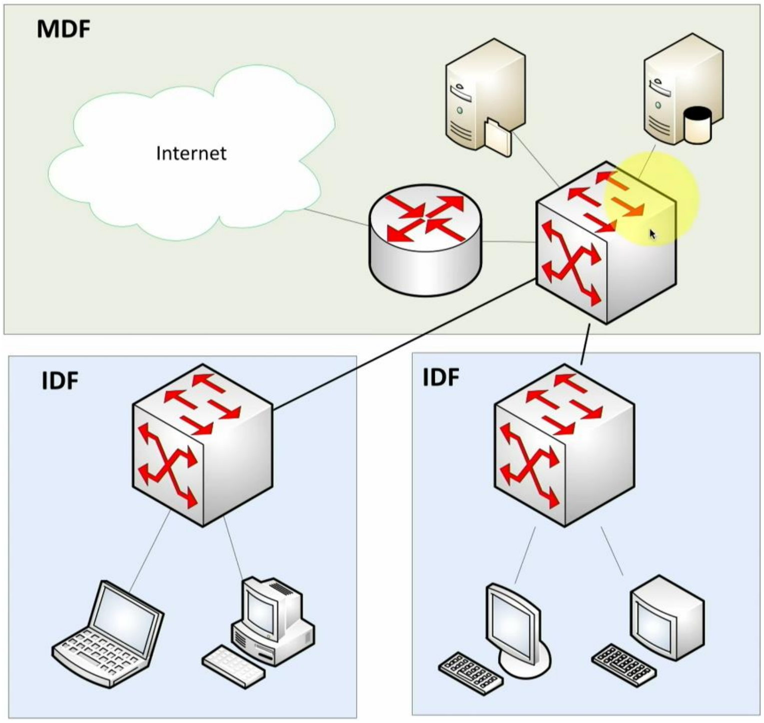
The other distribution frame you'll usually find is the Intermediate Distribution Frame (IDF). This is an extension of the MDF & can be thought of as an auxiliary of the MDF, and is a place where you're able to bring your users & connect them into the main network. There are going to be uplinks from here to the MDF.

The IDF is usually where you'll have switches for a floor or workgroup and local resources or anything else that doesn't need to be in the center of the network. You will commonly see IDFs in medium to large-scale environments where you have users on different floors or in different buildings, or separated geographically.

Q: The network install is failing redundancy testing at the MDF. The traffic being transported is a mixture of multicast and unicast signals. Which of the following devices would BEST handle the rerouting caused by the disruption of service?

A: Layer 3 Switch

A layer 3 switch is the best option because in addition to its capability of broadcast traffic reduction, it provides fault isolation and simplified security management. This is achieved through the use of IP address information to make routing decisions when managing traffic between LANs. Multicast and unicast are layer 3 messaging flows, so you need a router or layer 3 switch to route them across the network.



A smart hub is a layer 1 device. A proxy server operates at layer 4, but would still require a router or layer 3 switch to route the traffic.

Index

Q: A company is having a new T1 line installed. Which of the following does this connection MOST likely terminate?

A: Demarcation Point

The telecom company usually terminates the circuits at the Main Distribution Facility (MDF) at the demarcation point.

In telephony, the demarcation point is the point at which the public switched telephone network ends and connects with the customer's on-premises wiring. It is the dividing line which determines who is responsible for installation and maintenance of wiring and equipment—customer/subscriber, or telephone company/provider. The demarcation point varies between countries and has changed over time.

Demarcation point is sometimes abbreviated as demarc, DMARC, or similar.

Q: You are working at the demarcation point between your network and the telecommunication service provider's network. Which of the following devices serves as the demarcation point between the two networks?

A: Smartjack

A smartjack is an intelligent network interface device (NID) that serves as the demarcation point between the telecommunication service provider's local loop and the customer's premise wiring. A smartjack provides more than just a termination for the connection of the wiring, but also may provide signal conversion, converting codes, and protocols to the type needed by the customer's equipment, as well as diagnostic capabilities.

Hiding Cables: Conduits vs Raised Floors vs Cable Trays

Q: A company is setting up a brand-new server room and would like to keep the cabling infrastructure out of sight but still accessible to the network administrators. Infrastructure cost is not an issue. Which of the following should be installed to meet the requirements?

A: Raised Floor

Raised floors allow the cabling to be placed under the floor, but still accessible to the network administrators. A conduit is a tube through which power or data cables pass.

Conduits are usually metal or plastic pipes, and it makes accessing the cables difficult when maintenance is going to be performed.

Cable trays are a mechanical support system that can support electrical cables used for power distribution, control, and communication. Cable trays can be installed on the ceiling or under the floor if you are using a raised floor system. If cable trays are installed in the ceiling, they can be difficult to reach and work on.

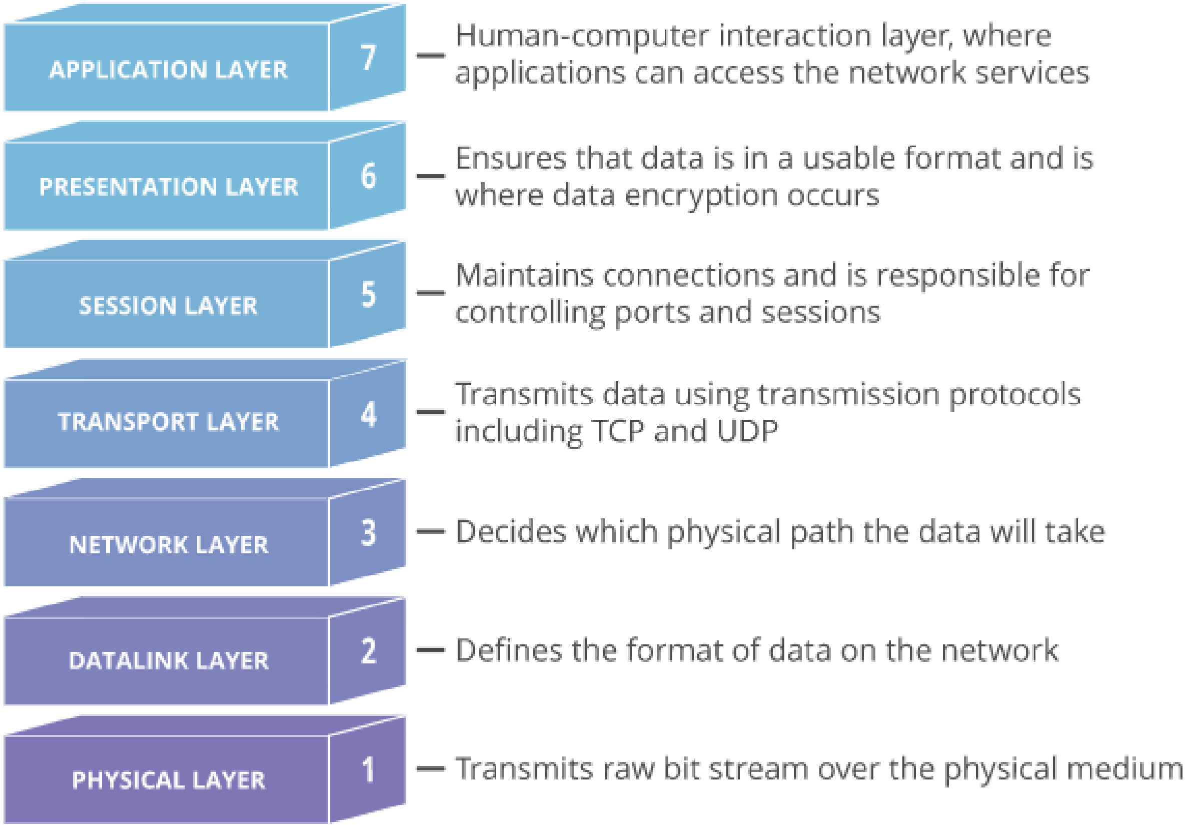
Networking

OSI Model

From CloudFlare.com

The Open Systems Interconnection model is a conceptual model created by the International Organization for Standardization and establishes a standard for computer communications over a network.

This model is comprised of 7 layers:



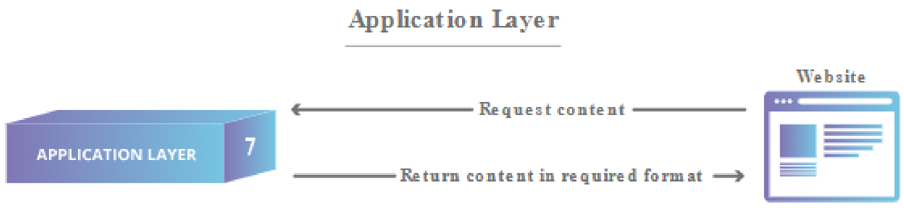
APPLICATION LAYER
7
Human-computer interaction layer, where applications can access the network services
PRESENTATION LAYER
6
Ensures that data is in a usable format and is where data encryption occurs
SESSION LAYER
5
Maintains connections and is responsible for controlling ports and sessions
TRANSPORT LAYER
4
Transmits data using transmission protocols including TCP and UDP
NETWORK LAYER
3
Decides which physical path the data will take
DATALINK LAYER
2
Defines the format of data on the network
PHYSICAL LAYER
1
Transmits raw bit stream over the physical medium

Why does the OSI model matter?

Although the modern Internet doesn't strictly follow the OSI Model (it more closely follows the simpler Internet protocol suite), the OSI Model is still very useful for troubleshooting network problems. Whether it's one person who can't get their laptop on the Internet, or a web site being down for thousands of users, the OSI Model can help to break down the problem and isolate the source of the trouble. If the problem can be narrowed down to one specific layer of the model, a lot of unnecessary work can be avoided.

Index

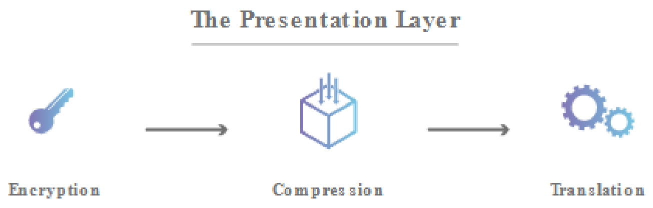
7. The Application Layer



This is the only layer that directly interacts with data from the user. Software applications like web browsers and email clients rely on the application layer to initiate communications. **But it should be made clear that client software applications are NOT a part of the application layer**; rather the application layer is responsible for the protocols and data manipulation that the software relies on to present meaningful data to the user. Application layer protocols include HTTP as well as SMTP (Simple Mail Transfer Protocol is one of the protocols that enables email communications).

Modern TCP/IP (approx.) Equivalent Protocols: HTTP, HTTPS, SMTP

6. The Presentation Layer



This layer is primarily responsible for preparing data so that it can be used by the application layer; in other words, layer 6 makes the data presentable for applications to consume. **The presentation layer is responsible for translation, encryption, and compression of data. Data encryption and character set conversion (such as ASCII to EBCDIC) are usually associated with this layer.**

Two communicating devices may be using different encoding methods, so layer 6 is responsible for translating incoming data into a syntax that the application layer of the receiving device can understand.

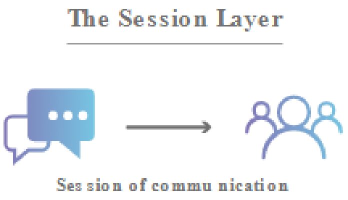
If the devices are communicating over an encrypted connection, layer 6 is responsible for adding the encryption on the sender’s end as well as decoding the encryption on the receiver's end so that it can present the application layer with unencrypted, readable data.

Finally, the presentation layer is also responsible for compressing data it receives from the application layer **before delivering it to layer 5**. This helps improve the speed and efficiency of communication by minimizing the amount of data that will be transferred.

Modern TCP/IP (approx.) Equivalent Protocols: MIME, SSL/TLS, XDR

Index

5. The Session Layer

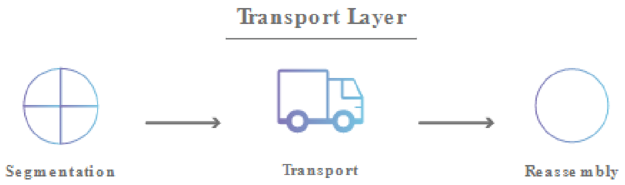


This is the layer responsible for opening and closing communication between the two devices. The time between when the communication is opened and closed is known as the session. The session layer **ensures that the session stays open long enough to transfer all the data being exchanged, and then promptly closes the session in order to avoid wasting resources**.

The session layer also synchronizes data transfer with checkpoints. For example, if a 100 MB file is being transferred, **the session layer could set a checkpoint every 5 megabytes**. In the case of a disconnect or a crash after 52 megabytes have been transferred, the session could be resumed from the last checkpoint, meaning only 50 more megabytes of data need to be transferred. Without the checkpoints, the entire transfer would have to begin again from scratch.

Modern TCP/IP (approx.) Equivalent Protocols: Sockets (session establishment in TCP/RTP/PPTP (Point-to-Point Tunneling Protocol)

4. The Transport Layer



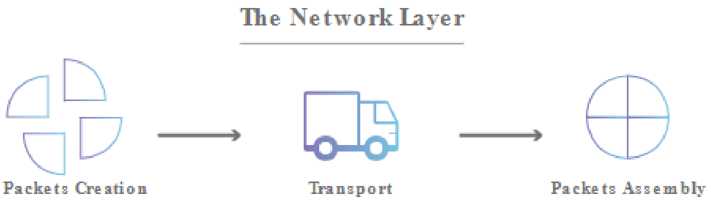
Layer 4 is **responsible for end-to-end communication** between the two devices. This includes taking data from the session layer and breaking it up into chunks called **segments** before sending it to layer 3. The transport layer on the receiving device is responsible for **reassembling** the segments into data the session layer can consume.

The transport layer is also responsible for **flow control and error control**. Flow control determines an optimal speed of transmission to ensure that a sender with a fast connection doesn't overwhelm a receiver with a slow connection. The transport layer performs error control on the receiving end by ensuring that the data received is complete and requesting a retransmission if it isn't.

Modern TCP/IP (approx.) Equivalent Protocols: TCP, UDP, SCTP, DCCP

Index

3. The Network Layer

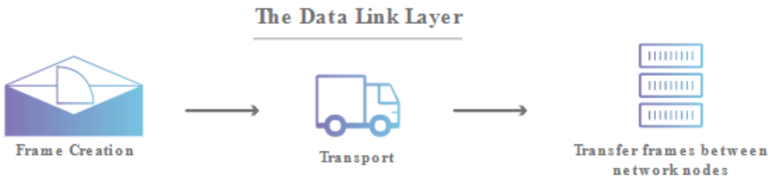


The network layer is responsible for facilitating data transfer **between two different networks**. If the two devices communicating are on the same network, then the network layer is unnecessary. The network layer **breaks up segments** from the transport layer into smaller units, called **packets**, on the sender's device, and **reassembles** these packets on the receiving device. The network layer also finds the **best physical path** for the data to reach its destination; this is known as **routing**.

Modern TCP/IP (approx.) Equivalent Protocols: IP, IPsec (used for VPNs), ICMP, IGMP, OSPF, RIP

Special Note: QoS occurs at layers 2 & 3: Layer 2 QoS allows for traffic prioritization and bandwidth management to minimize network delay using Cost of Service (CoS) classification, and DSCP marking under the 802.1p standard. Layer 3 Quality of Service (QoS) allows for managing the quality of network connections through its packet routing decisions.

2. The Datalink Layer



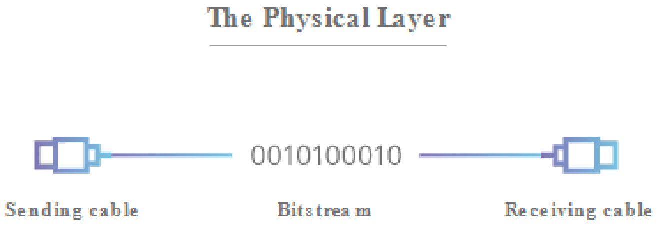
The data link layer is very similar to the network layer, except the data link **layer facilitates data transfer between two devices on the SAME network**. The data link layer takes **packets from the network layer and breaks them** into smaller pieces called **frames**. Like the network layer, the data link layer is **also responsible for flow control and error control in intra-network communication** (The transport layer only does flow control and error control for inter-network communications).

Modern TCP/IP (approx.) Equivalent Protocols: PPP, SBTV, SLIP

Special Note: The Neighbor Discovery Protocol (NDP) is an IPv6 technology that's part of the data-link layer of ISO-OSI and is responsible for gathering various information required for internet communication, including the configuration of local connections and the domain name servers and gateways used to communicate with more distant systems.

Index

1. The Physical Layer



This layer includes the **physical equipment** involved in the data transfer, such as the cables and switches. This is also the layer where the **data gets converted into a bit stream**, which is a string of 1s and 0s. The physical layer of both **devices must also agree on a signal convention** so that the 1s can be distinguished from the 0s on both devices.

Modern TCP/IP (approx.) Equivalent Protocols: N/A

How data flows through the OSI Model

In order for human-readable information to be transferred over a network from one device to another, the data must travel down the seven layers of the OSI Model on the sending device and then travel up the seven layers on the receiving end.

For example: Mr. Cooper wants to send Ms. Palmer an email. Mr. Cooper composes his message in an email application on his laptop and then hits ‘send’. His email application will pass his email message over to the application layer, which will pick a protocol (**SMTP**) and pass the data along to the presentation layer. The presentation layer will then **compress** the data and then it will hit the session layer, which will initialize the communication **session**.

The data will then hit the sender’s transportation layer where it will be segmented, then those **segments** will be broken up into **packets** at the network layer, which will be broken down even further into **frames** at the data link layer. The data link layer will then deliver those frames to the physical layer, which will convert the data into a **bitstream** of 1s and 0s and send it through a physical medium, such as a **cable**.

Once Ms. Palmer’s computer receives the bit stream through a physical medium (such as her Wi-Fi), the data will flow through the same series of layers on her device, but in the **opposite order**. First the physical layer will convert the bitstream of 1s and 0s into frames that get passed to the data link layer. The data link layer will then reassemble the frames into packets for the network layer. The network layer will then make segments out of the packets for the transport layer, which will reassemble the segments into one piece of data.

The data will then flow into the receiver's session layer, which will pass the data along to the presentation layer and then end the communication session. The presentation layer will then remove the compression and pass the raw data up to the application layer. The application layer will then feed the human-readable data along to Ms. Palmer’s email software, which will allow her to read Mr. Cooper’s email on her laptop screen.

Index

TCP/IP Model, AKA the Internet Protocol Suite

From Oracle Docs:

TCP/IP Protocol Architecture Model

The OSI model describes an idealized network communications with a family of protocols. TCP/IP does not correspond to this model directly. TCP/IP either combines several OSI layers into a single layer or does not use certain layers at all. The following table shows the layers of the Solaris implementation of TCP/IP. The table lists the layers from the topmost layer (application) to the lowest (physical network).

OSI Ref. Layer No.	OSI Layer Equivalent	TCP/IP Layer	TCP/IP Protocol Examples
5,6,7	Application, session, presentation	Application	HTTP, HTTPS, SMTP, SSL/TLS, Sockets, NFS, NIS+, DNS, telnet, ftp, rlogin, rsh, rcp, RIP, RDISC, SNMP, etc
4	Transport	Transport	TCP, UDP
3	Network	Internet	IP, ARP, ICMP
2	Data link	Data link	PPP, IEEE 802.2
1	Physical	Physical network	Ethernet (IEEE 802.3) Token Ring, RS-232, others

The table shows the TCP/IP protocol layers. Also shown are the OSI Model equivalents with examples of the protocols that are available at each level of the TCP/IP protocol stack. Each host that is involved in a communication transaction runs a unique implementation of the protocol stack.

Note on Data Flows in the OSI & TCP/IP Models

- Data is ENCAPSULATED as it moves DOWN from Layer 7 to Layer 1
- Data is DE-ENCAPSULATED as it moves UP from Layer 1 to Layer 7
- DO NOT MIX THE TWO!
- Remember it as getting ready to go to work and heading down an apartment building, and conversely stripping down bare immediately on returning home like any normal human does.

Index

Q: You are currently troubleshooting a network connection error. When you ping the default gateway, you receive no reply. You checked the default gateway & it's functioning properly, but the gateway cannot connect to any of the workstations on the network. Which of the following layers could be the issue?

A: Physical Layer

Ping requests occur at layer 3 (Network Layer). Therefore, the problem could exist in layer 1 (physical), layer 2 (data link), or layer 3 (network). Since Physical (layer 1) is the only choice from layers 1-3 given, it must be the correct answer. Also, since the gateway cannot reach any of the other devices on the network, it is most likely a cable (physical) issue between the gateway and the network switch.

Asynchronous Transfer Mode

Asynchronous Transfer Mode (ATM) is a telecommunications standard defined by the American National Standards Institute (ANSI) and the International Telecommunication Union - Telecommunication Standardization Sector (ITU-T; formerly CCITT) for digital transmission of multiple types of traffic. ATM was developed to meet the needs of the Broadband Integrated Services Digital Network as defined in the late 1980s, and designed to integrate telecommunication networks. It can handle both traditional high-throughput data traffic and real-time, low-latency content such as telephony (voice) and video. ATM provides functionality that uses features of circuit switching and packet switching networks by using asynchronous time-division multiplexing.

In the OSI reference model data link layer (layer 2), the basic transfer units are called frames. **In ATM these frames are of a fixed length (53 octets) called cells.** This differs from approaches such as Internet Protocol (IP) or Ethernet that use variable-sized packets or frames. **ATM uses a connection-oriented model** in which a virtual circuit must be established between two endpoints before the data exchange begins. These virtual circuits may be either permanent (dedicated connections that are usually preconfigured by the service provider), or switched (set up on a per-call basis using signaling and disconnected when the call is terminated).

The ATM network reference model **approximately maps to the three lowest layers of the OSI model**: physical layer, data link layer, and network layer. ATM is a core protocol used in the Synchronous Optical Networking and Synchronous Digital Hierarchy (SONET/SDH) backbone of the Public Switched Telephone Network (PSTN) and in the Integrated Services Digital Network (ISDN) but has largely been superseded in favor of next-generation networks based on IP technology. **Wireless and mobile ATM never established a significant foothold.**

Q: Your network relies on the use of ATM cells. At which layer of the OSI model do ATM cells operate?

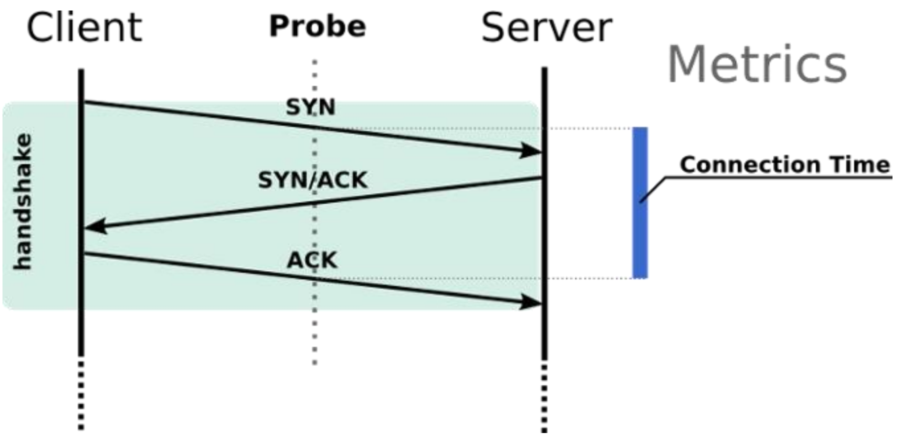
A: Data-Link Layer

TIP: ***-> Remember the OSI order of Segments -> Packets -> Frames as the 'SPF' of sunscreen lotions! Also logically: TCP Segments, IP Packets and Data Frames.***

-> Remember the equivalency of OSI Frames & ATM Cells as getting "framed" and put in a jail "cell"!

Index

TCP Handshake & Flags



Reset (RST) flag is used to terminate the connection. This type of **termination of the connection is used when the sender feels that something has gone wrong with the TCP connection** or that the conversation should not have existed in the first place. For example, if a system receives information that is outside of an established session, it will send an RST flag in response.

Finish (FIN) flag is used to request connection termination. This usually occurs at the end of a session and allows for the system to release any reserved resources set aside for communication.

Synchronization (SYN) flag is set in the **first** packet sent by the sender to a receiver as a means of establishing a TCP connection and initiating a three-way handshake. Once received, the receiver sends back a SYN with an Acknowledgement (ACK) flag set in a packet back to the initiator to confirm that they are ready to initiate the connection. Finally, the initial sender replies with an ACK flag set in a packet so that the three-way handshake can be completed, and data transmission can begin.

Frame Relay

Frame Relay is a WAN technology that specifies the physical and data link layers of digital telecommunications channels using a packet switching methodology. **It supports the use of virtual circuits and point-to-multipoint connections.** It is commonly used to connect multiple smaller corporate office locations back to a larger centralized headquarters.

Index

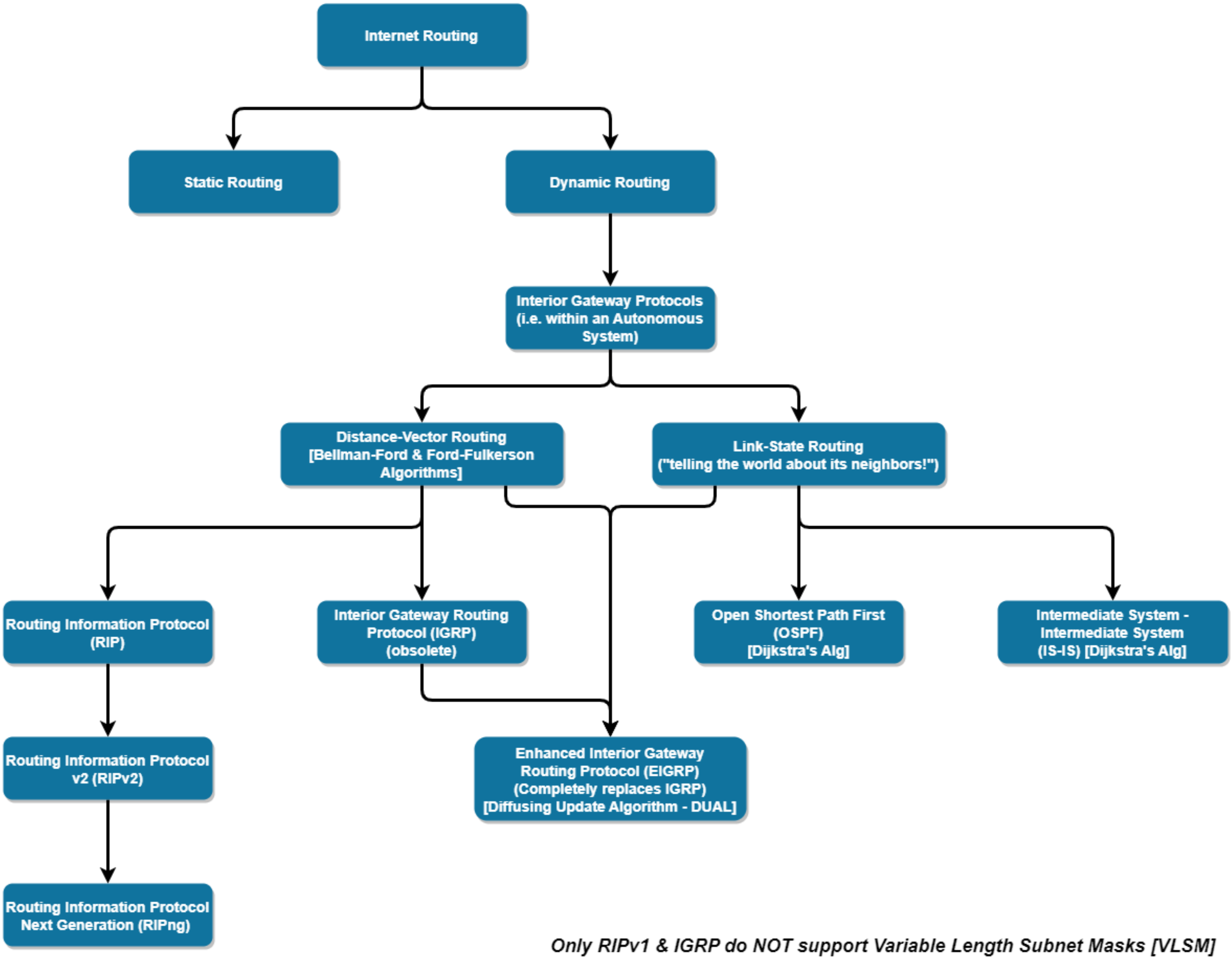
Routing

Static & Dynamic Routing Protocols

Static Routing is a form of routing wherein a router uses a manually configured routing entry, rather than dynamically routing traffic. Static routes are often **manually configured by a network-administrator** by adding entries into a routing table. Unlike dynamic routing, static routes are **fixed and do not change** even if the network physically changes or is reconfigured and must thus be re-routed manually to resolve issues. Nevertheless, most of the Public Switched Telephone Network (PSTN) uses pre-computed routing tables, with fallback routes if the most direct route becomes blocked.

Larger networks have complex topologies that can change rapidly, making the manual construction of routing tables unfeasible. Dynamic Routing attempts to solve this problem by constructing routing tables automatically, based on information carried by routing protocols, allowing the network to act nearly autonomously in avoiding network failures and blockages. Dynamic routing dominates the Internet. With dynamic routing, a router can automatically route traffic to another link or connection if any link goes down.

There are several protocols used for dynamic routing:


Internet Routing
Static Routing
Dynamic Routing
Interior Gateway Protocols (i.e. within an Autonomous System)
Distance-Vector Routing [Bellman-Ford & Ford-Fulkerson Algorithms]
Link-State Routing ("telling the world about its neighbors!")
Routing Information Protocol (RIP)
Interior Gateway Routing Protocol (IGRP) (obsolete)
Open Shortest Path First (OSPF) [Dijkstra's Alg]
Intermediate System - Intermediate System (IS-IS) [Dijkstra's Alg]
Routing Information Protocol v2 (RIPv2)
Enhanced Interior Gateway Routing Protocol (EIGRP) (Completely replaces IGRP) [Diffusing Update Algorithm - DUAL]
Routing Information Protocol Next Generation (RIPng)

Only RIPv1 & IGRP do NOT support Variable Length Subnet Masks [VLSM]

Both dynamic routing and static routing are usually used on a router to maximize routing efficiency and to provide backups in case dynamic routing information fails to be exchanged. Static routing can also be used in stub networks (a somewhat casual term describing a network with no knowledge of other networks that typically routes all non-local traffic out via a single known default route), or to provide a gateway of last resort (default gateway).

An Interior Gateway Protocol (IGP) or Interior routing protocol is a type of routing protocol used for exchanging routing table information between gateways (commonly routers) **within an autonomous system** (for example, a system of corporate local area networks). This routing information can then be used to route network-layer protocols like IP.

By contrast, Exterior Gateway Protocols are used to exchange routing information **between autonomous systems and rely on IGPs** to resolve routes within an autonomous system. Notable exterior gateway protocols include Exterior Gateway Protocol (EGP), now obsolete, and **Border Gateway Protocol (BGP).**

Border Gateway Protocol (BGP) is classified as a **Path-Vector Routing Protocol**, and it makes routing decisions based on paths, network policies, or rule-sets configured by a network administrator. BGP used for routing within an autonomous system is called Interior Border Gateway Protocol, **Internal BGP (iBGP)** (typically occurs within very large organizations such as Facebook or Microsoft). In contrast, the Internet application of the protocol is called Exterior Border Gateway Protocol, **External BGP (eBGP)**.

In BGP, the Autonomous System Boundary Routers (ASBR) send path-vector messages to advertise the reachability of networks. Each router that receives a path vector message must verify the advertised path according to its policy. If the message complies with its policy, the router modifies its routing table and the message before sending the message to the next neighbor.

A Path-Vector Routing Protocol is a network routing protocol which maintains the path information that gets updated dynamically. Updates that have looped through the network and returned to the same node are easily detected and discarded. This algorithm is sometimes used in Bellman–Ford routing algorithms to avoid "Count to Infinity" problems. It is different from the distance vector routing and link state routing. Each entry in the routing table contains the destination network, the next router, and the path to reach the destination.

A Distance-Vector Routing Protocol **determines the best route for data packets based on distance**: DVRPs measure the distance by the number of routers a packet has to pass, with one router counting as one hop. Some distance-vector protocols also take into account network latency and other factors that influence traffic on a given route. To determine the best route across a network, routers using DVRPs exchange information with one another, usually **routing tables plus hop counts for destination networks** and possibly other traffic information. DVRPs also require that a router inform its neighbors of network topology changes periodically.

The Routing Information Protocol (RIP) is one of the oldest distance-vector routing protocols which employs hop count as a routing metric. RIP prevents routing loops by implementing a limit on the number of hops allowed in a path from source to destination. The hop-limit is 15, which limits the size of networks that RIP can support. RIP implements the split horizon, route poisoning, & holddown mechanisms to prevent propagation of incorrect routing information. In RIPv1, routers broadcast updates to their routing table every 30 seconds.

RIPv2 included the ability to carry subnet information, thus supporting Classless Inter-Domain Routing (CIDR). To maintain backward compatibility, the hop count limit of 15 remained. In an effort to avoid unnecessary load on hosts that do not participate in routing, RIPv2 multicasts the entire routing table to all adjacent routers at the address 224.0.0.9, as opposed to RIPv1 which uses broadcast. Unicast addressing is still allowed for special applications. Route tags were also added in RIPv2: this allows a distinction between routes learned from the RIP protocol and routes learned from other protocols.

RIPng (RIP Next Generation) is an extension of RIPv2 for support of IPv6. RIPng does not support RIPv1 updates authentication, while RIPv2 does.

Interior Gateway Routing Protocol (IGRP) is a **proprietary** distance vector interior gateway protocol (IGP) developed by Cisco. IGRP was created in part to overcome the limitations of RIP (maximum hop count of only 15, & a single routing metric) when used within large networks. IGRP is considered a classful routing protocol.

Because the protocol has no field for a subnet mask, the router assumes that all subnetwork addresses within the same Class A, B, or C network have the same subnet mask as that configure for the interfaces. This contrasts with classless routing protocols that can use Variable Length Subnet Masks (VLSM). Classful protocols have become less popular as they are wasteful of IP address space.

Enhanced Interior Gateway Routing Protocol (EIGRP) is an advanced **proprietary** distance-vector routing protocol developed by Cisco, **initially available only on Cisco routers**. In 2013 Cisco decided to allow other vendors freely implement limited version of EIGRP with some of its associated features such as High Availability (HA), while withholding other EIGRP features such as EIGRP stub, needed for Dynamic Multipoint Virtual Private Network (DMVPN) and large-scale campus deployment, exclusively for themselves. EIGRP replaced the Interior Gateway Routing Protocol (IGRP) in 1993. One of the major reasons for this was the change to **classless** IPv4 addresses in the Internet Protocol, which IGRP could not support.

Link-State Routing Protocols are another way of determining the best routes across a network and are based on calculating "link costs": the basic concept here is that every node constructs a map of the network connectivity, in the form of a graph, thus determining node connections. Each node then independently calculates the next best logical path from itself to every possible destination in the network. Each collection of best paths will then form each node's own routing table. The protocol is performed by every switching node (router) in the network.

This contrasts with distance-vector routing protocols, which work by having each node share its routing table with its neighbors, in a link-state protocol the only information passed between nodes is connectivity related. Link-state algorithms are sometimes characterized informally as each router, "telling the world about its neighbors": *In link-state routing protocols,* ***each router possesses information about the complete network topology****. Each router then independently calculates the best next hop from it for every possible destination in the network using local information of the topology.* ***The collection of best-next-hops forms the routing table.***

Open Shortest Path First (OSPF) is based on the Shortest Path First (SPF) algorithm: it gathers link state information from available routers and constructs a topology map of the network. The topology is presented as a routing table to the Internet Layer which routes packets based solely on their destination IP address. OSPF supports Internet Protocol Version 4 (IPv4) and Internet Protocol Version 6 (IPv6) networks and supports the Classless Inter-Domain Routing (CIDR) addressing model, i.e. it support VLSM.

Index

Asymmetric Routing is when network packets leave via one path and return via a different path (unlike symmetric routing, in which packets come and go using the same path).

A Missing Route occurs when the dynamic or static routes in a router do not contain a route needed for specific traffic being routed.

Q: An organization has hired you to upgrade its wired computer network. The network currently uses static routing for the internal network, but the organization wants to reconfigure it to use a dynamic routing protocol. The new dynamic routing protocol must support both IPv4 and VLSM. Based on the requirements provided, which of the following routing protocols should you enable and configure?

A: OSPF

Only OSPF supports IPv4 and VLSM (Variable Length Subnet Mask) from the options provided in this question: VRRP, RIPv1, and HSRP do not support VLSM.

Virtual Router Redundancy Protocol (VRRP)

The Virtual Router Redundancy Protocol (VRRP) is a computer networking protocol that provides for automatic assignment of available Internet Protocol (IP) routers to participating hosts. This increases the availability and reliability of routing paths via automatic default gateway selections on an IP subnetwork.

The protocol achieves this by the creation of virtual routers, which are an **abstract representation of multiple routers**, i.e. primary/active and secondary/standby routers, acting as a group. The virtual router is assigned to act as a default gateway of participating hosts, instead of a physical router. If the physical router that is routing packets on behalf of the virtual router fails, another physical router is selected to automatically replace it. The physical router that is forwarding packets at any given time is called the primary/active router.

VRRP provides information on the state of a router, not the routes processed and exchanged by that router. Each VRRP instance is limited, in scope, to a single subnet. It does not advertise IP routes beyond that subnet or affect the routing table in any way. VRRP can be used in Ethernet, MPLS and Token Ring networks with Internet Protocol Version 4 (IPv4), as well as IPv6.

Hot Standby Router Protocol (HSRP)

In computer networking, the Hot Standby Router Protocol (HSRP) is a Cisco proprietary redundancy protocol for establishing a **fault-tolerant default gateway**. Version 2 of the protocol includes improvements and supports IPv6 but there is no corresponding RFC published for this version.

The protocol establishes an association between gateways in order to achieve default gateway failover if the primary gateway becomes inaccessible. HSRP gateways send **multicast** hello messages to other gateways to notify them of their priorities (which gateway is preferred) and current status (active or standby).

Index

Holddown Mechanism

Holddown works by having each router start a timer when they first receive information about a network that is unreachable. Until the timer expires, the router will discard any subsequent route messages that indicate the route is in fact reachable. It can solve the case where multiple routers are connected indirectly. In other words, a holddown keeps a router from receiving route updates until the network appears to be stable—until either an interface stops changing state (**flapping**) or a better route is learned.

Convergence (Routing)

Convergence or routing convergence is a state in which a set of routers in a network share the same topological information. The routers in the network collect the topology information from one another through the routing protocol. Any change — for example, the failure of a device — in the network affects convergence until information about the change is propagated to all routers and convergence is achieved again. The time taken by the routers in the network to reach convergence after a change in topology is termed **convergence time**.

Q: What happens when convergence on a routed network occurs?

A: All routers learn the route to all connected networks

Routers exchange routing topology information with each other by using a routing protocol. When all routers have exchanged routing information with all other routers within a network, the routers have converged. In other words: All routers "agree" on what the network topology looks like. A Hold-Down Timer allows for the routers in a topology to have sufficient time to reach convergence and be updated when a route fails.

Routing with Labels - Multi-Protocol Label Switching (MPLS)

Multiprotocol Label Switching (MPLS) is a routing technique in telecommunications networks that directs data from one node to the next based on labels rather than network addresses. Whereas network addresses identify endpoints the labels identify established paths between endpoints. MPLS can encapsulate packets of various network protocols, hence the multiprotocol component of the name. MPLS supports a range of access technologies, including T1/E1, ATM, Frame Relay, and DSL. **MPLS uses point-to-point connections.**

Q: You have been asked to troubleshoot a router which uses label-switching and label-edge routers to forward traffic. Which of the following types of protocols should you be familiar with to troubleshoot this device?

A: MPLS

Index

Route Poisoning

Route poisoning is a method to prevent a router from sending packets through a route that has become invalid within computer networks. Distance-vector routing protocols in computer networks use route poisoning to indicate to other routers that a route is no longer reachable and should not be considered from their routing tables.

Split-Horizon Route Advertisement

A split-horizon route advertisement is a method of **preventing routing loops in distance-vector routing protocols** by prohibiting a router from advertising a route back onto the interface from which it was learned. Split-horizon does not prevent large routing tables, duplicate addresses, or network collisions, it only works to prevent routing loops.

Q: A network architect is designing a highly redundant network with a distance vector routing protocol to prevent routing loops. The architect wants to configure the routers to advertise failed routes with the addition of an infinite metric. What should the architect configure to achieve this?

A: Route Poisoning

<u>Route Poisoning</u> is a method to prevent a router from sending packets through a route that has become invalid within computer networks. This is achieved by changing the route's metric to a value that exceeds the maximum allowable hop count so that the route is advertised as unreachable.

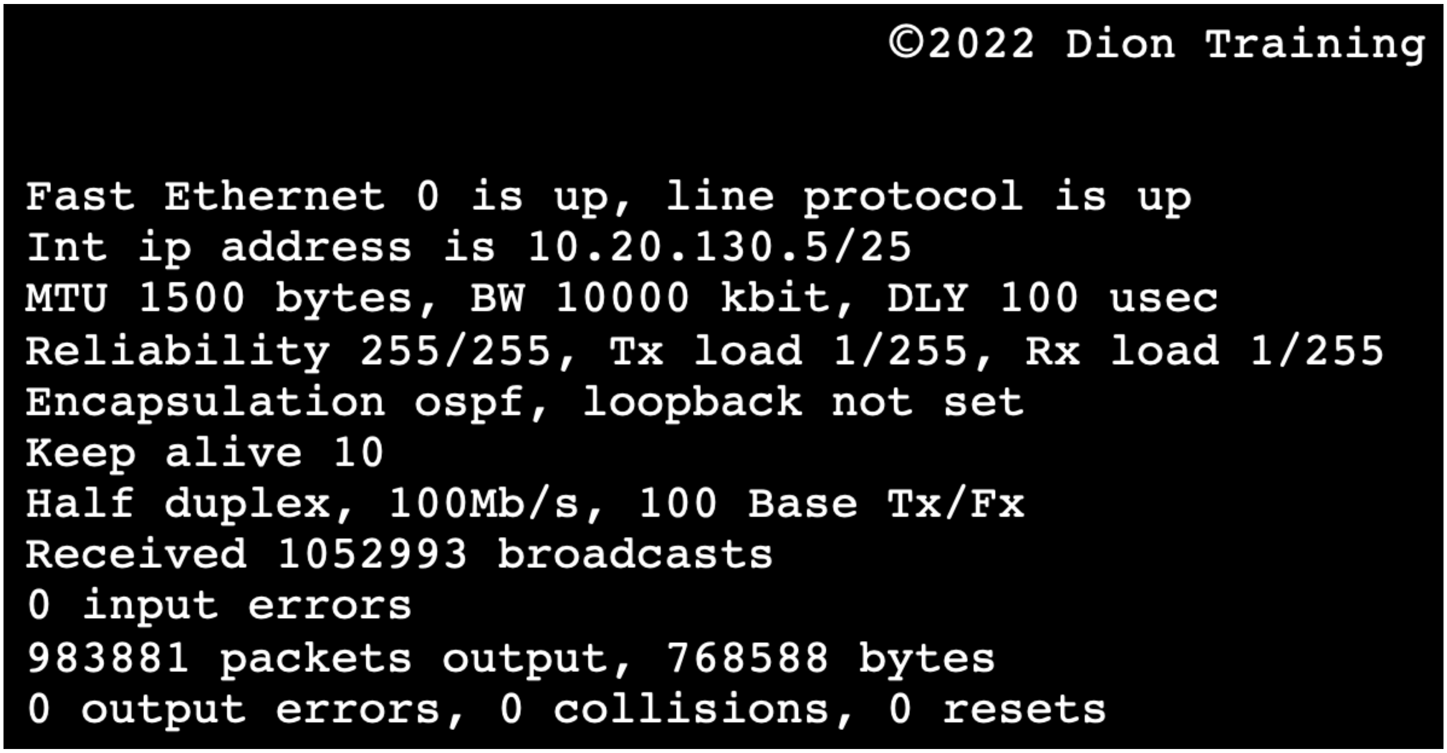
Q: A network engineer has been tasked with designing a network for a new branch office with approximately 50 network devices. This branch office will connect to the other offices via a MAN and using a router as their gateway device. Many of the other branch offices use off-the-shelf SOHO equipment. It is a requirement that the routing protocol chosen use the least amount of overhead. Additionally, all the computers on the network will be part of a single VLAN. The connection between these computers should produce the highest throughput possible in the most cost-effective manner. Which routing protocol should be used with the gateway router and what device should you select to connect the computers within the branch office?

A: RIPv2 as the routing protocol; connect the computers with a Gigabit Layer 2 switch

RIPv2 is a classless, distance vector routing protocol that will include the subnet mask with the network addresses in its routing updates. <u>RIPv2 has the least overhead of the four routing protocol options presented in this question (OSPF, EIGRP, RIPv2 and BGP).</u> If you were not sure about this, you could look at answering the second half of the question concerning the interconnection of the computers within the branch office instead and try to eliminate some of the wrong options. Due to the requirement of using the highest throughput, you can eliminate the 802.11n MIMO access point as it will have a maximum throughput of 600 Mbps and the other options are all 1000 Mbps/1Gbps. You can also eliminate the Fibre Channel switch since Fibre Channel is largely used to connect computers and servers to storage devices in a storage area network (SAN). At this point, you would have to choose between the layer 2 or layer 3 gigabit switch which are fairly equivalent for the purposes of this question but at least you have increased your odds of guessing the right answer from 25% to 50% by eliminating two wrong answer choices!

Index

Q: Dion Training's network is using OSPF for the internal routing protocol. One of the interfaces connected to the internet is congested. The data is going out to the internet slowly, but is frequently queued by the router prior to sending due to the congestion and lower than normal speeds. You entered the "show interface" command and received the following output:



```
                                  ©2022 Dion Training


Fast Ethernet 0 is up, line protocol is up
Int ip address is 10.20.130.5/25
MTU 1500 bytes, BW 10000 kbit, DLY 100 usec
Reliability 255/255, Tx load 1/255, Rx load 1/255
Encapsulation ospf, loopback not set
Keep alive 10
Half duplex, 100Mb/s, 100 Base Tx/Fx
Received 1052993 broadcasts
0 input errors
983881 packets output, 768588 bytes
0 output errors, 0 collisions, 0 resets
```

A: Change the duplex setting from half to full

Based on the output provided, the interface is set to half-duplex. Since there are no errors, collisions, or resets, the interface appears to be connected directly to another switchport or interface in their own collision domain. Therefore, the duplex can be set to full-duplex & this will effectively double the throughput on this interface. The loopback address on all interfaces is set to 127.0.0.1 by default, therefore there is no need to make this configuration change. The output shows "loopback not set", which indicates the interface is currently in production or operational mode. If the "loopback is set", this means the interface has a loopback plug installed and you are conducting diagnostics on the interface. The CIDR notation of /25 indicates a subnet with 126 usable hosts. If you modified the CIDR notation to use a classful subnet mask for a Class A network (10.0.0.0/8) it would create 16.7 million usable hosts in a single broadcast domain and would drastically slow down the network. The speed of the network is not influenced by whether a public or private IP address is used by the interface, therefore this is an incorrect option.

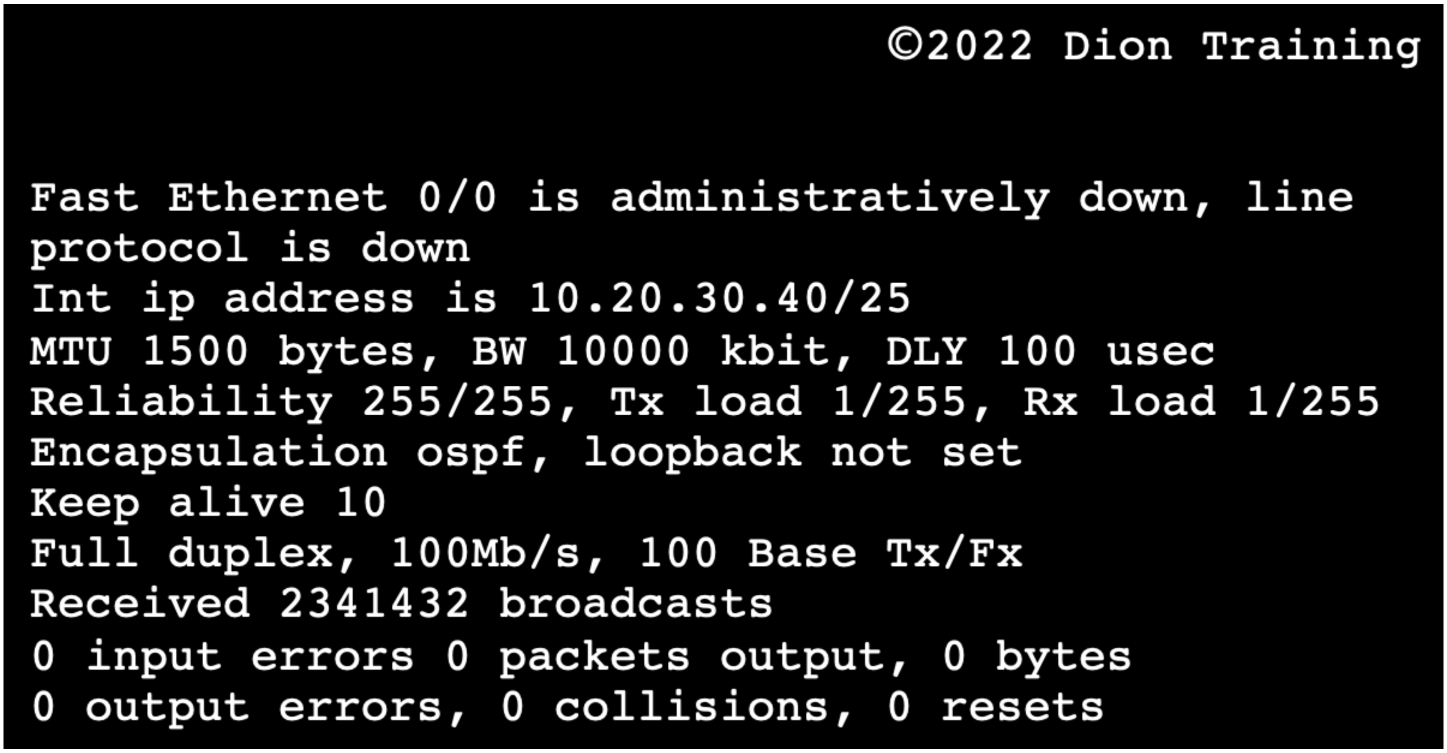
Q: Which of the following network issues can be prevented by configuring the split-horizon options on your network devices?

A: Routing Loops

A split-horizon route advertisement is a method of preventing routing loops in distance-vector routing protocols by prohibiting a router from advertising a route back onto the interface from which it was learned. Split-horizon does not prevent large routing tables, duplicate addresses, or network collisions, it only works to prevent routing loops.

Index

Q: An administrator’s router with multiple interfaces uses OSPF as its routing protocol. You have discovered that one of the router’s interfaces is not passing traffic. You enter the “show interface eth 0/0” command at the CLI and receive the following output:



```
                                    ©2022 Dion Training


Fast Ethernet 0/0 is administratively down, line
protocol is down
Int ip address is 10.20.30.40/25
MTU 1500 bytes, BW 10000 kbit, DLY 100 usec
Reliability 255/255, Tx load 1/255, Rx load 1/255
Encapsulation ospf, loopback not set
Keep alive 10
Full duplex, 100Mb/s, 100 Base Tx/Fx
Received 2341432 broadcasts
0 input errors 0 packets output, 0 bytes
0 output errors, 0 collisions, 0 resets
```

A: Verify the cable is connected to eth 0/0 and Enable the switchport for eth 0/0

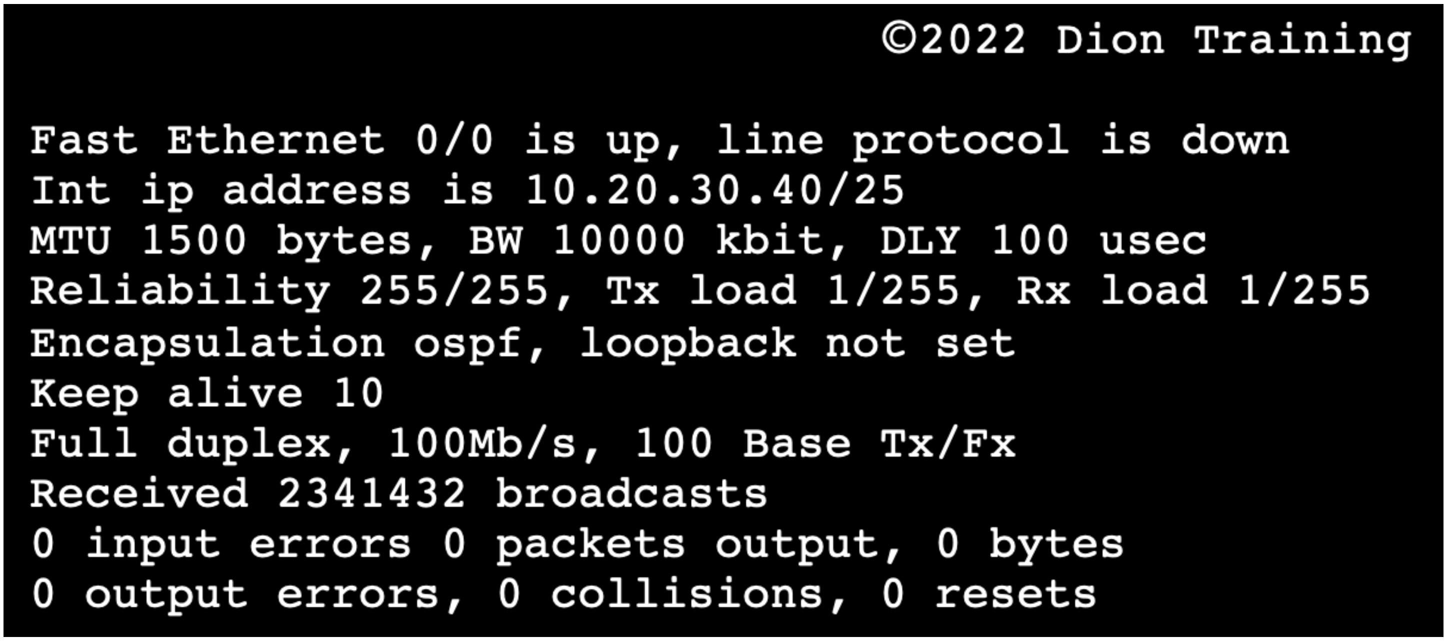
The key to answering this question is the first line of the output. "The line protocol is down" means that the specified interface has been correctly configured & enabled, but the Ethernet cable might be disconnected from the switchport. The line protocol being down indicates a clocking or framing problem on the connection, and the most common reason for this is a patch cable that is not properly connected. “Fast Ethernet 0/0 is administratively down” indicates that the switchport was manually shut down using the shutdown command by a network administrator and would need to be reenabled. The IP address is currently set to 10.20.30.40/25 which is a private IP address in a classless subnet range. As long as the default gateway is an IP between 10.20.30.0 and 10.20.30.127, though, there is nothing wrong with using this IP address. Without knowing the default gateway, we cannot identify the IP address as the issue. The “loopback is not set” indicates that the interface is not in diagnostic mode and should be properly sending traffic instead of sending it to a loopback address or port.

Q: Tim, a network administrator, is configuring a test lab that consists of three routers using RIP for dynamic routing. He connects the routers in a full mesh topology. When he attempts to ping Router 1 from Router 3 using its IP address, he receives a "Destination Unreachable" error message. Which of the following is the most likely reason for the connectivity error?

A: Split-Horizon is misconfigured: With split horizon, if a router receives routing information from another router, the first router will not broadcast that information back to the second router, thus preventing routing loops from occurring. If it is misconfigured, the routers could suffer a routing loop which would produce the error message received when trying to communicate with each other

Index

Q: An administrator’s router with multiple interfaces uses OSPF as its routing protocol. You have discovered that one of the router’s interfaces is not passing traffic. You enter the “show interface eth 0/0” command at the CLI and receive the following output:



```
                                           ©2022 Dion Training

Fast Ethernet 0/0 is up, line protocol is down
Int ip address is 10.20.30.40/25
MTU 1500 bytes, BW 10000 kbit, DLY 100 usec
Reliability 255/255, Tx load 1/255, Rx load 1/255
Encapsulation ospf, loopback not set
Keep alive 10
Full duplex, 100Mb/s, 100 Base Tx/Fx
Received 2341432 broadcasts
0 input errors 0 packets output, 0 bytes
0 output errors, 0 collisions, 0 resets
```

A: Verify the cable is connected to eth 0/0

The key to answering this question is the first line of the output that states the line protocol is down. This means that the specified interface has been correctly configured and enabled, but the Ethernet cable might be disconnected from the switchport. The line protocol being down indicates a clocking or framing problem on the connection, and the most common reason for this is a cable that is not properly connected. If “Fast Ethernet 0/0 is administratively down”, this would have indicated that the switchport was manually shut down using the shutdown command by a network administrator and would need to be reenabled. But, since “Fast Ethernet 0/0 is up”, this indicates the interface was already enabled for eth 0/0. The IP address is currently set to 10.20.30.40/25 which is a private IP address in a classless subnet range. As long as the default gateway is an IP between 10.20.30.0 and 10.20.30.127, though, there is nothing wrong with using this IP address. Without knowing the default gateway, we cannot identify the IP address as the issue. The “loopback is not set” indicates that the interface is not in diagnostic mode and should be properly sending traffic instead of sending it to a loopback address or port.

Routing VPN Connections Across Geographically Dispersed Sites

Q: Dion Training is trying to connect two geographically dispersed offices using a VPN connection. You have been asked to configure their networks to allow VPN traffic into the network. Which device should you configure FIRST?

A: Firewall

You should FIRST configure the firewall since the firewall is installed at the network's external boundary (perimeter). By allowing the VPN connection through the firewall, the two networks can be connected and function as a single intranet (internal network). After configuring the firewall, you will need to verify the router is properly configured to route traffic between the two sites using the site-to-site VPN connection.

Index

Network Models / Topologies

A Hub-and-Spoke Network, aka Star Network, is a network topology where each individual piece of a network is attached to a central node, such as a switch, i.e. a central component/device (the switch/hub) is connected to multiple networks/devices around it (the spokes). **It's the most popular network topology used on LANs.**

A Mesh Network **connects every node directly to every other node**. It's a network in which devices & nodes are linked together, branching off to other devices & nodes. This creates a **highly efficient, resilient, and redundant network**, but it is **expensive** to build and maintain. Larger mesh networks may include multiple routers, switches, and other devices, which operate as nodes. A mesh network can include hundreds of wireless mesh nodes, which allows it to span a large area. Examples: IoT & Metropolitan networks (MANs) with various network infrastructure.

A Bus Topology is a network topology in which nodes are directly connected to a common network media, such as a coaxial cable, known as the bus. Thus, **a single cable connects all the included nodes** and the main cable acts as a backbone for the entire network. Example: pure Ethernet networks.

A Ring Topology is a network topology in which each node connects to exactly two other nodes, forming a single continuous pathway for signals through each node to form a circular ring. Messages in a ring topology travel in one direction and usually **rely on a token to control the flow** of information. **Not often found today as it's largely replaced by the Star Network topology.**

A Peer-to-Peer Network Model does not differentiate between the clients and the servers, and every node can become a client and a server when requesting and responding to service requests.

A Point-to-Point Connection provides a path from one communication endpoint to another.

A Hybrid Topology is a kind of network topology that is a combination of two or more network topologies, such as mesh topology, bus topology, and ring topology.

A Client-Server Network Model utilizes specific devices (servers) to provide services to requesters (clients). **A server is a specialized computer that runs a networking operating system.** A client is any device that requests services over a network, such as a desktop, laptop, tablet, or internet of things device.

A Domain is a Microsoft client/server network model that groups computers together for security and to centralize administration. Domain members have access to a central user account database so that users can log on to any computer within the domain.

A Workgroup is a Microsoft peer-to-peer network model in which computers are connected together with access to shared resources for organizational purposes.

The Hub-and-Spoke and Mesh networking models are not used for workgroups or domains.

Q: Which of the following type of network models requires the use of specialized computers that utilize networking operating systems to provide services to other networked devices that request services from them over an enterprise network?

A: Client-Server

Index

Q: Which of the following network topologies requires that all nodes have a point-to-point connection with every other node in the network?

A: Mesh

Q: You are trying to select the BEST network topology for a new network based on the following requirements. The design must include redundancy using a minimum of two cables to create the network. The network should not be prone to congestion; therefore each device must wait for its turn to communicate on the network by passing around a token. Which of the following topologies would BEST meet the client's requirements?

A: Ring

Q: Dion Worldwide has recently built a network to connect four offices around the world together. Each office contains a single centralized switch that all of the clients connect to within that office. These switches are then connected to two of the other locations using a direct fiber connection between each office. The office in New York connects to the London office, the London office connects to the Hong Kong office, the Hong Kong office connects to the California office, and the California office connects to the New York office. Which of the following network topologies best describes the Dion Worldwide network?

A: Hybrid Topology

The WAN connections are using a ring network topology, but each office is using a star topology. Therefore, the best description of this combined network is a hybrid topology.

Q: Which of the following network topologies uses a single network device as a centralized node that all other devices connect back to in order to form the network?

A: Star

Multipoint GRE (mGRE)

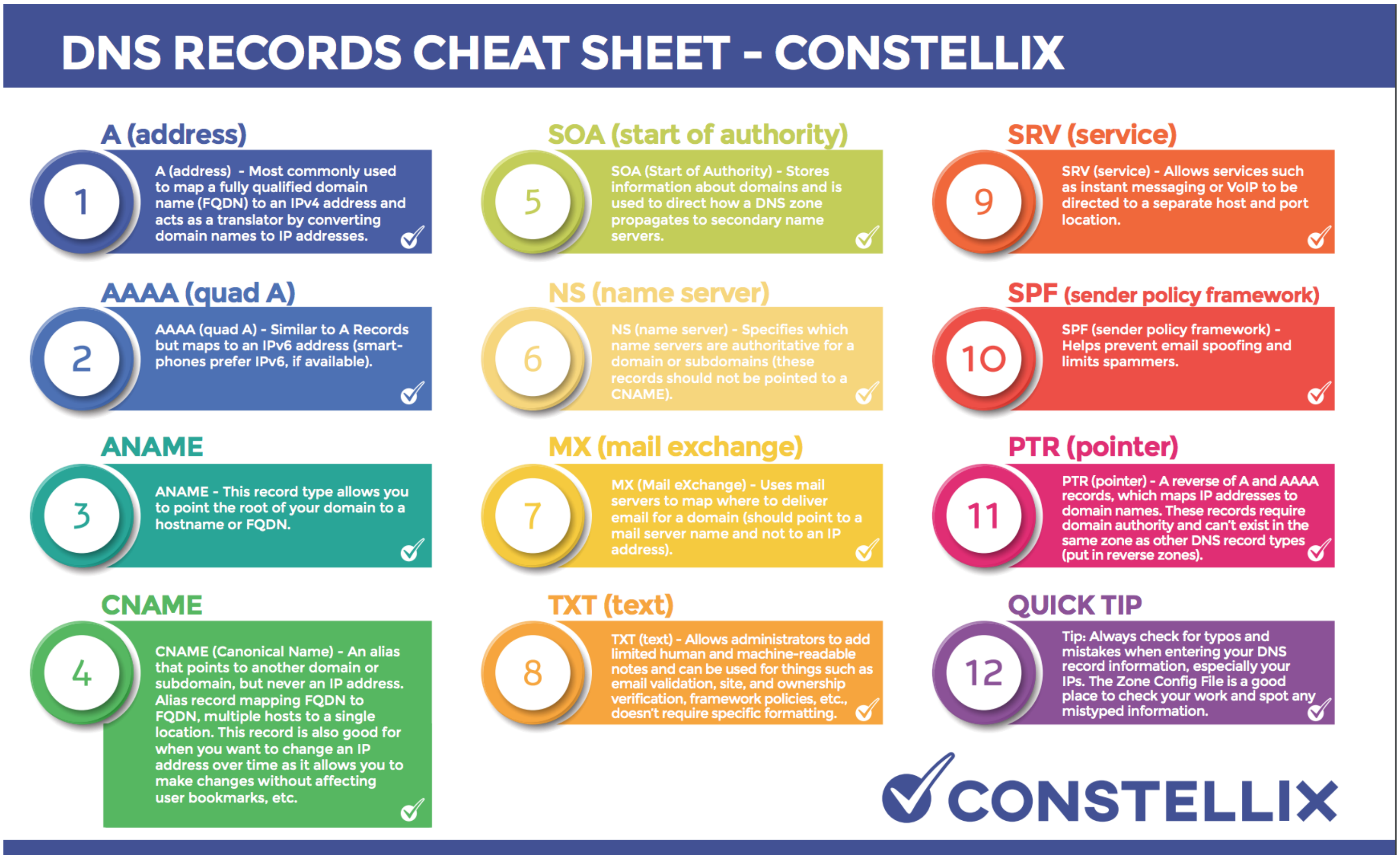
Multipoint Generic Routing Encapsulation or mGRE, is a protocol that can be used to enable one node to communicate with many nodes by encapsulating layer 3 protocols to create tunnels over another network. The mGRE protocol is often used in Dynamic Multipoint VPN (DMVPN) connections.

Q: Which of the following is often used to allow one node to communicate with many other nodes, such as in DMVPN connections?

A: mGRE

Index

DNS Record Types



DNS RECORDS CHEAT SHEET - CONSTELLIX

A (address)

1 A (address) - Most commonly used to map a fully qualified domain name (FQDN) to an IPv4 address and acts as a translator by converting domain names to IP addresses. ✓

AAAA (quad A)

2 AAAA (quad A) - Similar to A Records but maps to an IPv6 address (smart-phones prefer IPv6, if available). ✓

ANAME

3 ANAME - This record type allows you to point the root of your domain to a hostname or FQDN. ✓

CNAME

4 CNAME (Canonical Name) - An alias that points to another domain or subdomain, but never an IP address. Alias record mapping FQDN to FQDN, multiple hosts to a single location. This record is also good for when you want to change an IP address over time as it allows you to make changes without affecting user bookmarks, etc. ✓

SOA (start of authority)

5 SOA (Start of Authority) - Stores information about domains and is used to direct how a DNS zone propagates to secondary name servers. ✓

NS (name server)

6 NS (name server) - Specifies which name servers are authoritative for a domain or subdomains (these records should not be pointed to a CNAME). ✓

MX (mail exchange)

7 MX (Mail eXchange) - Uses mail servers to map where to deliver email for a domain (should point to a mail server name and not to an IP address). ✓

TXT (text)

8 TXT (text) - Allows administrators to add limited human and machine-readable notes and can be used for things such as email validation, site, and ownership verification, framework policies, etc., doesn't require specific formatting. ✓

SRV (service)

9 SRV (service) - Allows services such as instant messaging or VoIP to be directed to a separate host and port location. ✓

SPF (sender policy framework)

10 SPF (sender policy framework) - Helps prevent email spoofing and limits spammers. ✓

PTR (pointer)

11 PTR (pointer) - A reverse of A and AAAA records, which maps IP addresses to domain names. These records require domain authority and can't exist in the same zone as other DNS record types (put in reverse zones). ✓

QUICK TIP

12 Tip: Always check for typos and mistakes when entering your DNS record information, especially your IPs. The Zone Config File is a good place to check your work and spot any mistyped information. ✓

CONSTELLIX

A CNAME record is a canonical name or alias name, which associates one domain name as an alias of another (like beta.diontraining.com and www.diontraining.com could refer to the same website using a CNAME).

An ANAME record maps the root of your domain to a Fully Qualified Domain Name (FQDN) aka hostname.

An MX record is used for outgoing (SMTP) and incoming (POP3/IMAP) traffic.

An A record associates your domain name with an IPv4 address.

An AAAA record associates your domain name with an IPv6 address.

PTR records are used for the Reverse DNS lookup: using the IP address, you can get the associated domain/hostname. An A record should exist for every PTR record.

The text (TXT) record lets a domain administrator enter text into the Domain Name Systems. The TXT record was originally intended as a place for human-readable notes. However, now it is also possible to put some machine-readable data into TXT records. TXT records are a ***key component of several different email authentication methods*** *(Sender Policy Framework i.e. SPF, DKIM, and DMARC) that help an email server determine if a message is from a trusted source.*

A service (SRV) record specifies a host & port for specific services such as voice over IP (VoIP), instant messaging, etc.

Nameserver (NS) records are used to list the authoritative DNS server for a specified domain.

A Start of Authority (SOA) resource record indicates which DNS server is the best source of information for the specified domain.

Index

Q: While troubleshooting, a technician notices that some clients using FTP still work and that pings to the local routers and servers are working. The technician tries to ping all known nodes on the network, and they reply positively, except for one of the servers. The technician notices that ping works only when the hostname is used but not when FQDN is used. What server is MOST likely offline?

A: DNS Server

Split-View DNS

In computer networking, Split-Horizon DNS (also known as Split-View DNS, Split-Brain DNS, or **Split DNS** is the facility of a Domain Name System (DNS) implementation to **provide different DNS information, usually based on the source address of the requestor.**

This facility can provide a mechanism for security and privacy management by logical or physical separation of DNS information for **internal-network access** (within an administrative domain, e.g., company) and access from an unsecure, public network (e.g. the Internet).

Implementation of Split DNS can be accomplished with hardware-based separation or by software solutions. Hardware-based implementations run distinct DNS server devices for the desired access granularity within the networks involved. Software solutions use either multiple DNS server processes on the same hardware or special server software with the built-in capability of discriminating access to DNS zone records. The latter is a common feature of many server software implementations of the DNS protocol and is sometimes the implied meaning of the term since all other forms of implementation can be achieved with any DNS server software.

One common use case for Split-Horizon DNS is when a server has both a private IP address on a LAN (not reachable from most of the Internet) and a public address reachable across the Internet. By using split-horizon DNS the same name can lead to either the private IP address or the public one, depending on which client sends the query. This allows for critical local client machines to access a server directly through the local network, without the need to pass through a router. Passing through fewer network devices **improves the network latency.**

Q: A technician just completed a new external website and set up an access control list on the firewall. After some testing, only users outside the internal network can access the site. The website responds to a ping from the internal network and resolves the proper public address. What can the technician do to fix this issue while causing internal users to route to the website using its internal IP address?

A: Implement a Split-Horizon or Split-View DNS

Index

Network Parameters & Delays

Jitter is a network condition that occurs when a **time delay** occurs in sending data packets over a network connection. Jitter is a big problem for any real-time applications you may be supporting on your networks, like video conferences, voice-over IP, and virtual desktop infrastructure clients. A jitter is simply a variation in the delay of the packets, and this can cause some strange side effects, especially for voice and video calls. If you have ever been in a video conference where someone was speaking and then their voice started speeding up for 5 or 10 seconds, then returned to normal speed, you have been on the receiving end of their network's jitter.

Latency is the measure of time that it takes for data to reach its destination across a network. Usually, we measure network latency as the **round-trip time** from a workstation to the distant end and back.

Throughput is an **actual measure** of how much data is successfully transferred from the source to a destination.

Bandwidth is the maximum rate of data transfer across a given network. Now, bandwidth is more of a **theoretical concept** that measures how much data could be transferred from a source to a destination under ideal conditions. Therefore, we often measure throughput, instead of bandwidth, to monitor our network performance.

Crosstalk is defined as an effect caused by the unintentional and undesired transmission or **signal leakage** from one cable to another. Abused cables that are stepped/runover repeatedly can suffer from this.

An Optical Link Budget is a calculation that considers all the anticipated losses along the length of a fiber optic connection. Signal loss across a fiber optic cable occurs naturally due to the distance of the cable, as well as from losses due to multiplexing, bends in the cable, imperfect connections, patches, or splices along the fiber optic cable. If the circuit is designed with a low optical link budget and subsequently needs to be repaired or spliced, it would create a fiber connection that becomes too weak to pass the light across the entire fiber optic cable.

A Giant is any ethernet frame that exceeds the 802.3 frame size of 1518 bytes.

A Runt is an ethernet frame that is less than 64 bytes in size.

Index

Cellular Technology

3G Cellular Technology is made up of two different technologies: **HSPA+** (Evolved High-Speed Packet Access) *and* **EV-DO** (Evolution-Data Optimized)

- HSPA+ has a theoretical download speed of 168 Mbps and a theoretical upload speed of 34 Mbps. In the real world, though, HSPA+ normally reaches speeds around 20 Mbps.
- EV-DO is a 3G standard used for CDMA cellular networks and can support up to 3.1 Mbps downloads.
- **CDMA** was only popular in the United States with a few providers (Verizon and Sprint). Most of the world uses **GSM** instead.

4G Cellular Technology is made up of **LTE** *and* **LTA-A***:*

- LTE has a theoretical speed of 150 Mbps and a real-world speed of around 20 Mbps. LTE-Advanced (LTE-A) has a theoretical speed of 300 Mbps and a real-world speed of around 40 Mbps.

5G Cellular Technology is made up of three different types: **low-band, mid-band, and high-band mmWave (millimeter wave)** technology.

Index

Security

Threat & Attack Types

“A risk results from the combination of a threat and a vulnerability.”

A Zero-Day Vulnerability is an unknown vulnerability, so a patch or virus definition has not been released yet. A zero-day vulnerability refers to a hole in software that is unknown to the vendor. Hackers then exploit this security hole before the vendor becomes aware and hurries to fix it. This exploit is therefore called a zero-day attack. Such attacks include infiltrating malware, spyware, or allowing unwanted access to user information.

Rogue Anti-Virus (Scareware) is a form **of malicious software** and internet fraud that misleads users into believing there is a virus on their computer and to pay money for a fake malware removal tool (that actually introduces malware to the computer). It is a form of Scareware that manipulates users through fear and a form of ransomware. *If the alert is displayed on a macOS system but appears to be meant for a Windows system, it is obviously a scam or fake alert and most likely a rogue anti-virus attempting to infect the system!*

Worms are standalone malware programs that **replicates themselves** to spread to other computers. Often, they use a computer network to spread, relying on security failures on the target computer to access it.

Virus: Similar to a worm, but a worm can spread on its own whereas a virus **needs a host program** or user interaction to propagate itself. May be programmed to carry out malicious actions, such as deleting files or changing system settings.

A Trojan is a type of malware that looks legitimate but can take control of your computer. A Trojan is designed to damage, disrupt, steal, or in general, inflict some other harmful action on your data or network. To operate, a trojan will create numerous processes that run in the background of the system.

A Remote Access Trojan (RAT) is the most common form of a trojan, which allows an attacker to control a workstation or steal information remotely.

Missing Patches are the most common vulnerability found on both Windows and Linux systems. When a security patch is released, attackers begin to reverse engineer the security patch to exploit the vulnerability. If your servers are not patched against the vulnerability, they can become victims of the exploit, and the server's data can become compromised.

Cross-Site Scripting (XSS) attacks are a type of **injection** in which malicious scripts are injected into otherwise benign and trusted websites. Cross-site scripting focuses on exploiting a user’s workstation, not a server. If your website's HTML code does not perform input validation to remove scripts that may be entered by a user, then an attacker can create a popup window that collects passwords and uses that information to compromise other accounts further. Example: Submitting SQL code into an un-sanitized user form.

A Cross-Site Request Forgery (CSRF) is an attack that forces an end user to execute unwanted actions on a web application in which they are currently authenticated. An XSS will allow an attacker to execute arbitrary JavaScript within the victim's browser (such as creating pop-ups). A CSRF would allow an attack to induce a victim to perform actions they do not intend to perform. Think of it as cookie stealing and misuse.

Index

An Insider Threat is a type of threat actor assigned privileges on the system that cause an **intentional or unintentional** incident. Insider threats can be used as **unwitting** pawns of external organizations or make crucial mistakes that can open up exploitable security vulnerabilities.

A Rootkit is a set of software tools that enable an unauthorized user to control a computer system without being detected. A rootkit is a clandestine computer program designed to provide continued privileged access to a computer while actively hiding its presence. A rootkit is generally a collection of tools that enabled administrator-level access to a computer or network. They can often disguise themselves from detection by the operating system and anti-malware solutions. If a rootkit is suspected on a machine, it is best to reformat and reimage the system.

CRLF Injection is a software application **coding vulnerability** that occurs when an attacker injects a CRLF character sequence where it is not expected. The term CRLF refers to **Carriage Return (ASCII 13, \r) Line Feed (ASCII 10, \n).** They're used to note the termination of a line, however, dealt with differently in today's popular Operating Systems. For example: in Windows both a CR and LF are required to note the end of a line, whereas in Linux/UNIX a LF is only required. In the HTTP protocol, the CR-LF sequence is always used to terminate a line.

A CRLF Injection attack occurs when a user manages to submit a CRLF into an application. This is most commonly done by modifying an HTTP parameter or URL. Depending on how the application is developed, this can be a minor problem or a fairly serious security flaw.

Elaborating on the latter, let's assume a file is used at some point to read/write data to a log of some sort. If an attacker managed to place a CRLF, then can inject some sort of programmatic read method to the file. This could result in the contents being written to screen on the next attempt to use this file.

Another example is the "response splitting" attacks, where CRLFs are injected into an application and included in the response. The extra CRLFs are interpreted by proxies, caches, and maybe browsers as the end of a packet, causing mayhem.

SQL Injection is the placement of malicious code in SQL statements via web page input. SQL is commonly used against databases, but they are not useful when attacking file servers.

ARP Spoofing is a type of attack in which a malicious actor sends falsified ARP (Address Resolution Protocol) messages over a local area network. This results in the linking of an attacker's MAC address with the IP address of a legitimate computer or server on the network.

(The Address Resolution Protocol (ARP) is a communication protocol used for discovering the link layer address, such as a MAC address, associated with a given internet layer address, typically an IPv4 address. This mapping is a critical function in the Internet protocol suite.)

IP Spoofing is the creation of Internet Protocol (IP) packets that have a modified source address to either hide the identity of the sender, impersonate another computer system, or both.

Session Hijacking, also known as TCP Session Hijacking, is a method of taking over a web user session by surreptitiously obtaining the session ID and masquerading as the authorized user. This attack compromises the session token by stealing or predicting a valid session token to gain unauthorized access to the webserver.

A Distributed Denial-of-Service (DDoS) attack occurs when multiple systems flood the bandwidth or resources of a targeted system, usually one or more web servers.

Index

A Denial-of-Service (DoS) attack is a cyber-attack in which the perpetrator seeks to make a machine or network resource unavailable to its intended users by temporarily or indefinitely disrupting the services of a host connected to the Internet.

A Reflective DNS attack is a two-step attack used in DDoS attacks. The attacker sends a large number of requests to one or more legitimate DNS servers while using a spoofed source IP of the targeted victim. The DNS server then replies to the spoofed IP and unknowingly floods the targeted victim with responses to DNS requests that it never sent.

Evil Twin: An evil twin is **meant to mimic a legitimate hotspot** provided by a nearby business, such as a coffee shop that provides free Wi-Fi access to its patrons. An evil twin is a type of rogue wireless access point that masquerades as a legitimate Wi-Fi access point so that an attacker can gather personal or corporate information without the user's knowledge. This type of attack may be used to steal the passwords of unsuspecting users by monitoring their connections or phishing, which involves setting up a fraudulent website and luring people there.

Rogue Access Point: A rogue AP is an access point **installed on a network without the network owner's permission**. For example, if an employee connected a wireless access point to a wall jack in their office so that they can use their smartphone or tablet, this would be considered a rogue access point.

A Rogue DHCP Server is a DHCP server set up on a network by an attacker, or by an unaware user, and is not under the control of network administrators. Rogue DHCP servers are also commonly used by attackers for the purpose of network attacks such as an on-path or man-in-the-middle attack.

Wardialing (or War Dialing) is a technique to automatically scan a list of telephone numbers, **usually dialing every number in a local area code** to search for modems, computers, bulletin board systems (computer servers) and fax machines. Hackers use the resulting lists for various purposes: hobbyists for exploration, and crackers for guessing user accounts (by capturing voicemail greetings), or **locating modems** that might provide an entry-point into computer or other electronic systems. It may also be used by security personnel, for example, to detect unauthorized devices, such as modems or faxes, on a company's telephone network.

An On-Path Attack (previously known as a Man-in-the-Middle Attack) is a general term when a perpetrator positions himself in a conversation between a user and an application, either to eavesdrop or impersonate one of the parties, making it appear as if a normal exchange of information is occurring. For example, if your user and server are both in the United States (English language), but the attacker is performing the on-path attack from Russia, then the server will utilize the Russian language in the text since it sees the connection coming from a Russian IP address.

A Wi-Fi Deauthentication Attack is a type of denial-of-service attack that targets communication between a user and a Wi-Fi wireless access point by sending a deauthentication frame to the victim's machine.

VLAN Hopping is an attack where the attacker is able to send traffic from one VLAN into another by either double tagging the traffic or conducting switch spoofing. The main goal here is to gain access to other VLANs. There are two primary methods of VLAN hopping: **switch spoofing** and **double tagging.**

In a Switch Spoofing Attack, an attacking host imitates a trunking switch by speaking the tagging and trunking protocols (e.g. Multiple VLAN Registration Protocol, IEEE 802.1q, Dynamic Trunking Protocol) used in maintaining a VLAN. Traffic for multiple VLANs is then accessible to the attacking host. Switch spoofing can only be exploited when interfaces are set to negotiate a trunk.

Index

In a Double Tagging Attack, an attacker connected to an 802.1Q-enabled port prepends two VLAN tags to a frame that it transmits. The frame (externally tagged with VLAN ID that the attacker's port is really a member of) is forwarded without the first tag because it is the native VLAN of a trunk interface. The second tag is then visible to the second switch that the frame encounters. This second VLAN tag indicates that the frame is destined for a target host on a second switch. The frame is then sent to the target host as though it originated on the target VLAN, effectively bypassing the network mechanisms that logically isolate VLANs from one another. However, possible replies are not forwarded to the attacking host (**unidirectional flow**). Double Tagging can only be exploited on switch ports configured to use native VLANs: Trunk ports configured with a native VLAN don't apply a VLAN tag when sending these frames which allows an attacker's fake VLAN tag to be read by the next switch.

Index

Social-Engineering Attacks

Phishing is an **email-based social engineering attack** in which the attacker sends an email from a supposedly reputable source, such as a bank, to try to elicit private information from the victim. Phishing attacks target an indiscriminate large group of random people.

Vishing, aka "Voice Phishing", is the criminal practice of using social engineering over a telephone system to gain access to private personal and financial information from the public for the purpose of financial reward. It is also employed by attackers for reconnaissance purposes to gather more detailed intelligence on a target organization.

Smishing is the act of using SMS text messaging to lure victims into a specific course of action.

Pretexting is a type of social engineering attack that involves a situation, or pretext, created by an attacker in order to lure a victim into a vulnerable situation and to trick them into giving private information, specifically information that the victim would typically not give outside the context of the pretext. In its history, pretexting has been described as the first stage of social engineering, and has been used even by authorities to aid in investigations. A specific example of pretexting is reverse social engineering, in which the attacker tricks the victim into contacting the attacker first.

Impersonation: Pretending or pretexting to be another person with the goal of gaining access physically to a system or building. Impersonation is used in the "SIM swap scam" fraud.

Pharming / DNS Spoofing / DNS Poisoning is a type of **social engineering attack** that redirects a request for a website, typically an e-commerce site, to a similar-looking but **fake website**. The attacker uses DNS spoofing to redirect the user to the fake site.

Shoulder Surfing is a type of social engineering technique used to obtain information such as personal identification numbers, passwords, and other confidential data by looking over the victim's shoulder.

Piggybacking attack is a social engineering attempt by cyber threat actors in which they trick employees into helping them gain unauthorized access into the company premises.

Tailgating is when an unauthorized person physically follows an authorized person into a restricted corporate area or system.

The big difference between tailgating and piggybacking is permission: With tailgating, the authorized person doesn't know the unauthorized person is walking behind them. With Piggybacking, the authorized person will allow the unauthorized person to enter the secure area using the authorized person's access credentials.

Study tip for Piggybacking vs Tailgating - Think of a person attempting a Piggybacking attack: they’ll generally be very polite and sweet to get through and that’s why you may be fooled into allowing them in. Now think of a cute little piggy giving you the “oink oink” and not being able to resist taking it in! *Again, if it’s stupid but works…!*

Index

Anti-virus Software & Other Protection Suites

Heuristic Analysis is a method employed by many computer anti-virus programs designed to detect previously unknown computer viruses & new variants of viruses already in the wild. This is behavior-based detection & prevention, so it should detect previously unrecognized threats and stop them from spreading.

Host-based Intrusion Detection Systems (HIDS) are devices or software applications that monitor a system for malicious activity or policy violations. Any malicious activity or violation is typically reported to an administrator or collected centrally using a security information and event management system.

Unified Threat Management (UTM) Platforms enforce a variety of security-related measures, combining the work of a firewall, malware scanner, and intrusion detection/prevention. A UTM centralizes the threat management service, providing simpler configuration and reporting than isolated applications spread across several servers or devices.

Defense in Depth is an approach to cybersecurity in which a **series of defensive mechanisms are layered** to protect valuable data and information.

A Security Information and Event Management (SIEM) system provides real-time analysis of security alerts generated by applications and network hardware. SIEM is a term for software products and services combining security information management (SIM) and security event management (SEM). **A SIEM can consolidate syslog, SNMP, and event log data into a single repository.**

Q: Which type of antivirus scan provides the best protection for a typical home user?

A: On-access scans

On-access scans are a type of antivirus scan where the AV software intercepts operating system calls to open files to scan the file before allowing or preventing the file from being opened. On-access scans reduce performance somewhat but are essential to maintaining effective protection against malware. Weekly and daily scans are good to use, but they are not as effective in preventing infections as an on-access scan. A system administrator normally conducts safe mode scans after malware is found by an on-access, daily, or weekly scan.

Q: A corporate workstation was recently infected with malware. The malware was able to access the workstation's credential store and steal all the usernames and passwords from the machine. Then, the malware began to infect other workstations on the network using the usernames and passwords it stole from the first workstation. The IT Director has directed its IT staff to develop a plan to prevent this issue from occurring again. Which of the following would BEST prevent this from reoccurring?

A: Install an anti-virus or anti-malware solution that uses heuristic analysis

The only solution that could stop this from reoccurring would be to use an anti-virus or anti-malware solution with heuristic analysis. The other options (monitor SYSLOG server logs, install a HIDS or UTM) might be able to monitor and detect the issue but not stop it from spreading.

Index

Q: A network administrator, Tamera, follows the best practices to implement firewalls, patch management, and security policies on his network. Which of the following should be performed to verify that the security controls are in place?

A: Penetration Testing

Penetration testing or Pentesting is the practice of testing a computer system, network, or web application in order to find vulnerabilities that an attacker could exploit. It can be used to ensure all security controls are properly configured and in place.

Authentication, authorization, and accounting (AAA) is a term for a framework for intelligently controlling access to computer resources, enforcing policies, auditing usage, and providing the information necessary to bill for services. Testing AAA might be a part of a larger penetration test, but by itself it would not test the firewalls and patch management systems sufficiently.

A Disaster Recovery Test (DR test) is the examination of each step in a disaster recovery plan as outlined in an organization's business continuity/disaster recovery planning process. A disaster recovery test would not test the firewalls, patch management, or security policies.

A Single Point-of-Failure (SPOF) is a part of a system that, if it fails, will stop the entire system from working. A single point of failure test is used to identify a single point of failure in the network or system, and it is not designed to test the network's firewalls, patch management, or security policies.

Q: A network technician is selecting the best way to protect a branch office from as many different threats from the Internet as possible using a single device. Which of the following should meet these requirements?

A: Configure a UTM Device

Since this is a branch office and you want to protect it from as many threats as possible, using a Unified Threat Management (UTM) device would be <u>best</u> as a UTM will protect you from most things using a single device.

Q: Your workstation has fallen victim to an on-path attack. Upon investigation, you determine that the attack is occurring at layer 2 of the OSI model and is redirecting traffic destined for your workstation to the attackers' workstation instead. What type of attack was performed against your workstation?

A: ARP Spoofing

Index

Stateful vs Stateless Firewalls

Stateless firewalls are designed to protect networks based on static information such as source and destination. Whereas *stateful* firewalls filter packets based on the full context of a given network connection, stateless firewalls filter packets based on the individual packets themselves.

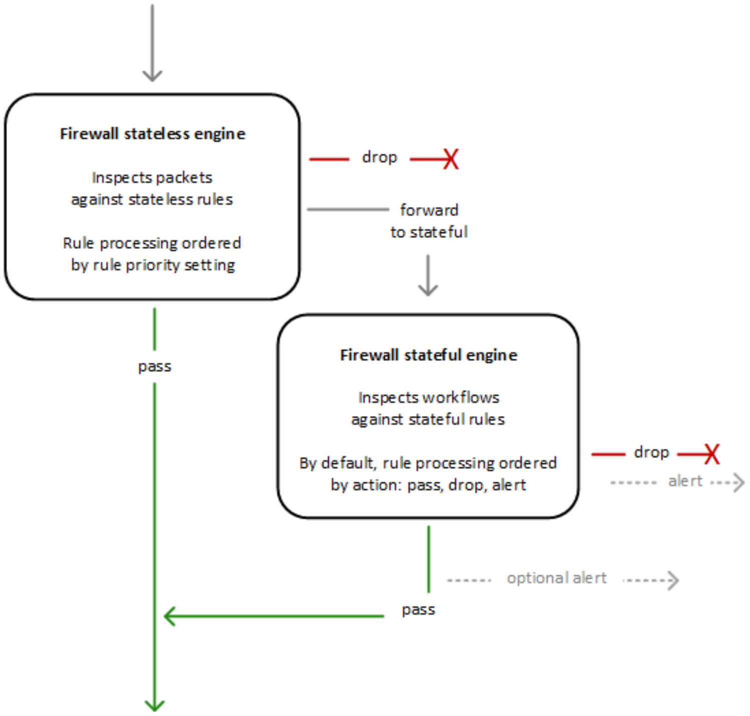
Stateless firewalls check individual packets before deciding whether or not to permit them, while stateful firewalls are able to track the movement of packets around a network, building profiles to better recognize safe & unsafe connections at the source.

Nice analogy by EnterpriseNetworkingPlanet: "*Firewalls are like club bouncers—they decide who gets in and stays out. Stateful firewalls are the experienced bouncer, who knows precisely who is coming and going and can recognize familiar faces. They keep track of all the connections that pass through them, ensuring that only authorized traffic is allowed to pass.*

Stateless firewalls, on the other hand, are the rookie bouncer who just checks ID at the door without keeping track of comings and goings. They don't recognize any connections and simply check each packet individually to see if it matches their predetermined ruleset."

Stateless rules engine – Inspects each packet in isolation, without regard to factors such as the direction of traffic, or whether the packet is part of an existing, approved connection. This engine prioritizes the speed of evaluation.

Stateful rules engine – Inspects packets in the context of their traffic flow, allows you to use more complex rules, and allows you to log network traffic and to log 'Network Firewall' firewall alerts on traffic. Stateful rules consider traffic direction. The stateful rules engine might delay packet delivery in order to group packets for inspection.

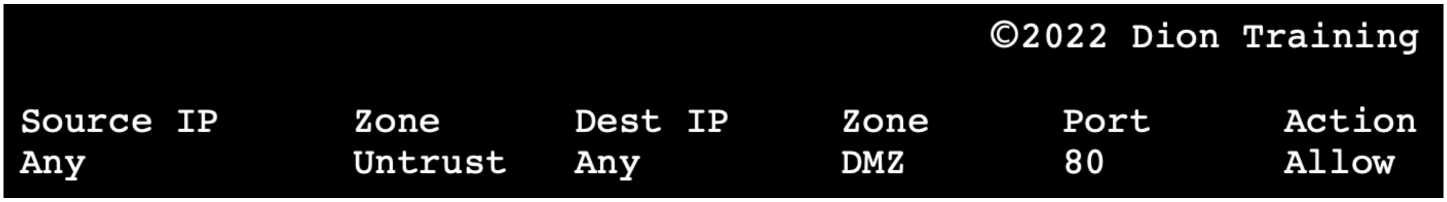

Firewall stateless engine
Inspects packets against stateless rules
Rule processing ordered by rule priority setting
drop
forward to stateful
pass
Firewall stateful engine
Inspects workflows against stateful rules
By default, rule processing ordered by action: pass, drop, alert
drop
alert
optional alert
pass

AWS Network Firewall – Rules Engine

Q: A network administrator needs to install a centrally located firewall that needs to block specific incoming and outgoing IP addresses without denying legitimate return traffic. Which type of firewall should the administrator install?

A: A Stateful Network-based Firewall

Q: A firewall technician at Dion Training configures a firewall to allow HTTP traffic as follows:



©2022 Dion Training

Source IP	Zone	Dest IP	Zone	Port	Action
Any	Untrust	Any	DMZ	80	Allow

Dion Training is afraid that an attacker might try to send other types of network traffic over port 80 to bypass their security policies. Which of the following should they implement to prevent unauthorized traffic from entering through the firewall?

A: Application-aware firewall

An application-aware firewall can make decisions about what applications are allowed or blocked by a firewall, as opposed to simply using IP addresses and port numbers, by applications by inspecting the data contained within the packets. A stateless packet inspection firewall allows or denies packets into the network based on the source and destination IP address or the traffic type (TCP, UDP, ICMP, etc.).

A stateful packet inspection firewall monitors the active sessions and connections on a network. The process of stateful inspection determines which network packets should be allowed through the firewall by utilizing the information it gathered regarding active connections as well as the existing ACL rules. Neither a stateless nor stateful inspection firewall operates at layer 6 or layer 7, so they cannot inspect the contents of the packet to ensure it contains HTTP traffic and nor other types of network traffic.

HTTPS (SSL/TLS) would allow for an encrypted communication path between the webserver and the client, but this would not prevent an attacker from sending other network protocol data over port 80 and bypassing the firewall rules.

Q: A new piece of malware attempts to exfiltrate user data by hiding the traffic and sending it over a TLS-encrypted outbound traffic over random ports. What technology would be able to detect and block this type of traffic?

A: Application-aware firewall

Q: Your deep packet inspection firewall is dropping portions of your packet flow as it enters or leaves the network. The network is configured to use HSRP to load balance traffic across two network devices in a high availability cluster. Which of the following issues would cause your network security devices, such as your firewalls, to drop packet flows and cause intermittent network connectivity to your clients?

A: Asymmetric Routing

Q:A network technician wants to allow HTTP traffic through a stateless firewall. The company uses the 192.168.0.0/24 network. Which of the following ACLs should the technician implement?

A: PERMIT SCRIP 192.168.0.0/24 SPORT: ANY DSTIP: ANY DPORT: 80

Wireless Network Security

WEP: The Wired Equivalent Privacy (WEP) encryption system **is based on the RC4 encryption cipher**. WEP uses a **40-bit encryption key and a 24-bit initialization vector by default, creating a 64-bit key**. Newer versions of WEP support a 128-bit key size. A larger encryption key creates stronger encryption and is more difficult to attack. WEP is **considered weak by today's standards** and should be replaced by WPA2 or strong encryption schemes.

WPA: Wi-Fi Protected Access (WPA) is an improved encryption scheme for protecting Wi-Fi communications designed to **replace WEP**. WPA uses the **RC4 cipher and a Temporal Key Integrity Protocol (TKIP)** to overcome the vulnerabilities in the older WEP protection scheme.

WPA2: Wi-Fi Protected Access 2 Pre-Shared Key or WPA2-PSK is a system of encryption used to authenticate users on wireless local area networks using a shared password as the key. WPA2-PSK [AES] is the recommended secure method of making sure no one can listen to your wireless data while it is being transmitted back and forth between your router and other devices on your network. WPA2 replaced the original version of WPA after the completion of the 802.11i security standard.

WPA2 features an improved method of key distribution and authentication for enterprise networks via WPA2 Enterprise, though the pre-shared key method is still available for home and small office networks via WPA2 Personal. WPA2 uses the **improved AES cipher with counter mode with Cipher-block Chaining Message Authentication Protocol (CCMP)** for encryption. WPA2 Enterprise requires a RADIUS authentication server to be used with individual usernames and passwords for each client, rather than a PSK.

WPA3: Wi-Fi protected access version 3 (WPA3) has **replaced WPA2 as the most secure** wireless encryption method. WPA3 uses the **Simultaneous Authentication of Equals (SAE)** password-based authentication & password-authenticated key agreement method to increase the security of pre-shared keys, and **replaces the 4-way handshake used in WPA-**based wireless networks. The SAE handshake is also known as the **dragonfly handshake**.

WPA3 provides an **enhanced open mode** that encrypts transmissions from a client to the access point when using an open network.

WPA3 Enterprise mode supports the use of AES with the Galois Counter Mode Protocol (GCMP-256) for the highest levels of encryption. AES GCMP is a high-performance mode of operation for symmetric encryption that supports **Authenticated Encryption with Associated Data (AEAD)**. Management protection frames protect unicast and multicast management action frames to protect against eavesdropping and forgery in WPA3-based wireless networks.

WPS: The Wi-Fi Protected Setup (WPS) is a **mechanism for auto-configuring a WLAN securely** for home users. On compatible equipment**, users push a button** on the access point and connect adapters to associate them securely. WPS is subject to brute force attacks against the PIN used to secure them, making them vulnerable to attack. The 8-digit PIN is susceptible to brute-force attacks as WPS, checks each half of the PIN individually, reducing the number of possible combinations from a maximum of 100,000,000 to only 11,000.

A WEP Attack is a **brute force password attack** conducted against a wireless network that relies on WEP for its encryption and security.

Index

Q: Which of the following encryption types was used by WPA to better secure wireless networks than WEP?

A: TKIP

Q: The administrator would like to use the strongest encryption level possible using PSK without utilizing an additional authentication server. What encryption type should be implemented?

A: WPA Personal or WPA2 Personal

Since he wishes to use a pre-shared key and not require an authentication server, WPA personal is the most secure choice. WPA2 Enterprise is incorrect since the requirement was for a PSK, whereas WPA2 Enterprise requires a RADIUS authentication server to be used with individual usernames and passwords for each client. MAC filtering does not use a password or pre-shared key (PSK). WEP uses a pre-shared key to secure a wireless network, but WPA uses a stronger encryption standard than WEP.

Q: Which attack utilizes a wireless access point made to look as if it belongs to the network by mimicking the corporate network's SSID to eavesdrop on the wireless traffic?

A: Evil Twin, as it's impersonating an official WAP by mimicking the SSID of the corporate network

Q: Joanne is having a drink at the coffee shop near her office. She takes out her Windows 10 laptop & connects it to the coffee shop's wireless network to check her email. Which type of network should she select to hide their computer from other devices on the network & prevent file sharing with other patrons?

A: Public

When connecting to a network for the first time, the user must select if it is a public or private network. A public network will hide your computer from other devices on the network & prevent file & printer sharing. A private network is considered trusted, allows the computer to be discoverable to other devices on the network, & supports the use of file & printer sharing. In older versions of Windows, there were also Home & Work network types, but those have since been merged into public & private network types, as well.

Least Privilege vs Zero-Trust

Least privilege is the concept and practice of **restricting access rights** for users, accounts, and computing processes to only those resources absolutely required to perform routine, legitimate activities.

Privilege itself refers to the authorization to bypass certain security restraints.

Zero-trust is a security framework that requires all users, whether in or outside the organization's network, to be authenticated, authorized, and **continuously validated** for security configuration and posture before being granted or keeping access to applications and data.

Index

Universal Plug-and-Play (UPnP) is a protocol framework allowing network devices to **autoconfigure** services, such as allowing a games console to request appropriate settings from a firewall. UPnP is associated with **several security vulnerabilities and is best disabled** if not required. You should ensure that the router does not accept UPnP configuration requests from the external (internet) interface. If using UPnP, keep up-to-date with any security advisories or firmware updates from the router manufacturer.

Geofences are a virtual perimeter for a real-world geographic area. Geofencing does not use shared passwords for security, it uses GPS coordinates or other location-based data.

Firewalls are a **network security device** that monitor & filter incoming & outgoing network traffic based on an organization's previously established security policies.

An Access Control List could define what ports, protocols, or IP addresses the ethernet port could be utilized.

Internet Protocol Security (IPsec) is a secure network protocol suite that authenticates and encrypts packets of data to provide secure, encrypted communication between two computers over an IP network. **It's used in VPNs.**

Q: Which protocol is used to establish a secure and encrypted VPN tunnel that can be initiated through a web browser?

A: SSL !

While IPsec is heavily used in VPNs, it's not used in browser-initiated ones! An SSL VPN is a type of virtual private network that uses the Secure Sockets Layer protocol in a standard web browser to provide secure, remote-access VPN capability. In modern browsers and servers, it is more common to use TLS (transport layer security) which is the successor to SSL.

The Point-to-Point Tunneling Protocol (PPTP) is an **obsolete method for implementing VPNs**. PPTP has many well-known security issues. PPTP uses a TCP control channel and a Generic Routing Encapsulation tunnel to encapsulate PPP packets. Many modern VPNs use various forms of UDP for this same functionality. The PPTP specification does not describe encryption or authentication features and relies on the Point-to-Point Protocol being tunneled to implement any and all security functionalities.

HMAC-based One-Time Password (HOTP) is a **one-time password algorithm** based on Hash-based Message Authentication Codes (HMAC).

Time-based One-Time Password (TOTP) is a computer algorithm that generates a **one-time password that uses the current time** as a source of uniqueness.

Proxy Servers: A proxy server is a **web server that acts as a gateway** between a client application. To route all of the workstation's internet traffic to the proxy server, a technician should configure the proxy server address under the Connections tab of the Internet Options section of the Control Panel.

Index

The Default Gateway parameter is the IP address of a router to which packets destined for a remote network should be sent by default.

The Subnet Mask is used to identify the host identifier and the network identifier uniquely in combination with the IP address. The subnet mask is used by the TCP/IP protocol to determine whether a host is on the local subnet or a remote network.

Q: You are configuring a Windows 10 Professional workstation to connect to the Dion Training domain. To provide additional security to its users, Dion Training requires that all uses route their internet traffic through a server located at 10.0.0.15 for inspection before it is sent to the internet. Once inspected, the server will route the traffic to the WAN router whose IP is 10.0.0.1. Which of the following settings should be configured on the workstation to achieve this?

A: Under Internet Options, configure the proxy server address as 10.0.0.15

The Internet Options section of the Control Panel allows a technician to manage the Internet settings for their computers, including the security settings, access settings, and add-on control settings. Using Internet Options, a technician can set the homepage of the browser, set up the proxy server connection details, and change the trust and security settings used by the system. Remember it as "IO" for input/output of traffic!

DHCP Snooping is a layer 2 security technology incorporated into the OS of a capable (managed) network switch that drops DHCP traffic determined to be unacceptable. This prevents unauthorized (rogue) DHCP server from offering IP addresses to clients. DHCP Snooping validates that DHCP messages are from trusted sources, building & maintaining a DHCP Snooping Binding Database of untrusted hosts with leased IP addresses, and utilizes that DB to validate subsequent requests from untrusted hosts.

Dynamic ARP Inspection (DAI) is a security feature that validates Address Resolution Protocol (ARP) packets in a network. DAI allows a network administrator to intercept, log, and discard ARP packets with invalid MAC address to IP address bindings.

Data loss Prevention (DLP) Software detects potential data breaches/data ex-filtration transmissions and prevents them by monitoring, detecting, and blocking sensitive data while in use (endpoint actions), in-motion (network traffic), and at rest (data storage).

Windows Internet Name Service (WINS) is a legacy computer name registration and resolution service that maps computer NetBIOS names to IP addresses.

Remote Authentication Dial-In User Service (RADIUS) is a networking protocol that provides centralized authentication, authorization, and accounting (AAA) management for users who connect and use a network service. RADIUS is an application-layer client/server protocol, with a server component usually running as a background process on UNIX or Windows.

Terminal Access Controller Access-Control System or TACACS+ is a AAA (accounting, authorization, and authentication) protocol **developed by CISCO** to provide AAA services for access to routers, network access points, & other networking devices. It's a remote authentication protocol, which allows a remote access server to communicate with an authentication server to validate user access onto the network. **TACACS+ allows a client to accept a username & password & pass a query to a TACACS+ authentication server.**

TACACS+ is an older username and login system that uses authentication to determine access, while RADIUS combines authorization AND authentication.

Q: Which of the following provides accounting, authorization, and authentication via a centralized privileged database, as well as challenge/response and password encryption?

A: TACACS+

Q: Your company wants to provide a secure SSO solution for accessing both the corporate wireless network and its network resources. Which of the following technologies should be used? And

Q: A company is installing several APs for a new wireless system that requires users to authenticate to the domain. The network technician would like to authenticate to a central point. What solution would be BEST to achieve this?

Answer to both: RADIUS

With RADIUS & SSO configured, users on the network can provide their user credentials one time when they initially connect to the wireless access point or another RADIUS client and are then automatically authenticated to all of the network's resources. The Remote Authentication Dial-in User Service (RADIUS) is used to manage remote & wireless authentication infrastructure. Users supply authentication information to RADIUS client devices, such as WAPs. The client device then passes the authentication data to an AAA server that processes the request. The Terminal Access Controller Access Control System (TACACS+) is a proprietary alternative to RADIUS developed by Cisco for handling authentication.

Q: A technician has finished configuring AAA on a new network device. However, the technician cannot log into the device with LDAP credentials but can with a local user account. What is the MOST likely reason for the problem?

A: Shared secret key is mismatched

AAA through RADIUS uses a Server Secret Key (a shared secret key). A secret key mismatch could cause login problems. A shared secret is a text string that serves as a password between hosts.

Kerberos is a network authentication protocol designed to provide strong mutual authentication for client/server applications using secret-key cryptography developed by MIT. Kerberos is a computer network authentication protocol that works **based on tickets** to allow nodes communicating over a non-secure network to prove their identity to one another in a secure manner. Kerberos is used in Windows Active Directory domains for authentication.

Challenge-Handshake Authentication Protocol (CHAP) is used to authenticate a user or network host to an authenticating entity. CHAP is an authentication protocol but does not provide authorization or accounting.

A DMZ (Demilitarized Zone), a type of screened subnet, is a physical or logical subnetwork that contains and exposes an organization's external-facing services to an untrusted network such as the Internet.

Index

Q: Your company has just installed a new web server that will allow inbound connections over port 80 from the internet while not accepting any connections from the internal network. You have been asked where to place the web server in the network architecture and configure the ACL rule to support the requirements. The current network architecture is segmented using a triple-homed firewall to create the following three zones: ZONE INTERFACE, IP address -------------------------------------- PUBLIC, eth0, 66.13.24.16/30 DMZ, eth1, 172.16.1.1/24 PRIVATE, eth2, 192.168.1.1/24 Based on the requirements and current network architecture above, where should you install the webserver and how should you configure it?

A: Put the server in the DMZ with an inbound rule from eth0 to eth1 that allows port 80 traffic to the server's IP

Q: Which of the following network devices would be considered a perimeter device and installed at the outermost part of the network?

A: Firewall

A Network Tap is used to create a physical connection to the network that sends a copy of every packet received to a monitoring device for capture and analysis.

Internet Security Association and Key Management Protocol (ISAKMP) is used for negotiating, establishing, modifying & deleting Security Association (SAs), cryptographic keys & related parameters in IPSec protocol.

Router Advertisement Guard: In an IPv6 deployment, routers periodically multicast Router Advertisement (RA) messages to announce their availability and convey information to neighboring nodes that enable them to be automatically configured on the network. RA messages are used by Neighbor Discovery Protocol (NDP) to detect neighbors, advertise IPv6 prefixes, assist in address provisioning, and share link parameters such as maximum transmission unit (MTU), hop limit, advertisement intervals, and lifetime. Hosts listen for RA messages for IPv6 address autoconfiguration and discovery of link-local addresses of the neighboring routers, and can also send a Router Solicitation (RS) message to request immediate advertisements.

RA messages are unsecured, which makes them susceptible to attacks on the network that involve the spoofing (or forging) of link-layer addresses. The IPv6 Router Advertisement Guard feature provides support for allowing the network administrator to block or reject unwanted or rogue router advertisement guard messages that arrive at the network device platform.

A Honeypot is a computer security mechanism set to detect, deflect, or, in some manner, counteract attempts at unauthorized use of information systems. Generally, a honeypot consists of data (for example, in a website) that appears to be a legitimate part of the site which contains information or resources of value to attackers. It is actually isolated, monitored, and capable of blocking or analyzing the attackers. This is similar to police sting operations, colloquially known as "baiting" a suspect. A honeypot is a single machine and cannot detect threats against an entire network.

A Remote Access Server (RAS) or remote desktop gateway is a type of server that provides a suite of services to connect users to a network or the Internet remotely.

The Domain Name System Security Extensions (DNSSEC) is a suite of extension specifications by the Internet Engineering Task Force for securing data exchanged in the Domain Name System in IP networks.

Index

Q: An organization wants to choose an authentication protocol that can be used over an insecure network without implementing additional encryption services. Which of the following protocols should they choose?

A: Kerberos

The Kerberos protocol is designed to send data over insecure networks while using strong encryption to protect the information. RADIUS, TACACS+, and PAP are all protocols that contain known vulnerabilities that would require additional encryption to secure them during the authentication process.

Q: The corporate network uses a centralized server to manage credentials for all of its network devices. What type of server is MOST likely being used in this configuration?

A: RADIUS or TACACS

Index

802.1X & Network Access Control (NAC)

IEEE 802.1X is an IEEE Standard for Port-based Network Access Control (PNAC). It is part of the IEEE 802.1 group of networking protocols. It provides an authentication mechanism to devices wishing to attach to a LAN or WLAN.

IEEE 802.1X defines the encapsulation of the Extensible Authentication Protocol (EAP) over wired IEEE 802 networks & over 802.11 wireless networks, which is known as "EAP over LAN" or EAPOL.

Extensible Authentication Protocol (EAP) is an authentication framework frequently used in network and internet connections. EAP is in wide use. For example, in IEEE 802.11 (Wi-Fi) the WPA and WPA2 standards have adopted IEEE 802.1X (with various EAP types) as the canonical (official) authentication mechanism.

802.1X authentication involves three parties: a supplicant (client device / software), an authenticator, and an authentication server:

1. The supplicant is a client device (such as a laptop) that wishes to attach to the LAN/WLAN. The term 'supplicant' is also used interchangeably to refer to the software running on the client that provides credentials to the authenticator.

2. The authenticator is a network device such as an Ethernet switch or wireless access point that provides a data link between the client and the network and can allow or block network traffic between them.

3. The authentication server supporting RADIUS & EAP protocols is a trusted server that can receive and respond to requests for network access, and can tell the authenticator if the connection is to be allowed, and various settings that should apply to that client's connection or setting. In some cases, the authentication server software may be running on the authenticator hardware.

Network Access Control (NAC) is an approach to computer security that attempts to unify endpoint security technology (such as antivirus, host intrusion prevention, and vulnerability assessment), user / system authentication and network security enforcement. **A basic form of NAC is the 802.1X standard.**

Network access control is a computer networking solution that uses a set of protocols to define and implement a policy that describes how to secure access to network nodes by devices when they initially attempt to access the network.

When a computer connects to a computer network, it is not permitted to access anything unless it complies with a business defined policy, including anti-virus protection level, system update level and configuration. NAC might integrate the automatic remediation process (fixing non-compliant nodes before allowing access) into the network systems, allowing the network infrastructure such as routers, switches, and firewalls to work together with back-office servers and end user computing equipment to ensure the information system is operating securely before interoperability is allowed.

Access to the network will be given according to the profile of the person and the results of a posture/health check. For example, in an enterprise the HR department could access only HR department files if both the role and the endpoint meet anti-virus minimums.

Index

Q: Dion Training allows its visiting business partners from CompTIA to use an available Ethernet port in their conference room to establish a VPN connection back to the CompTIA internal network. The CompTIA employees should obtain internet access from the Ethernet port in the conference room, but nowhere else in the building. Additionally, if any of the Dion Training employees use the same Ethernet port in the conference room, they should access Dion Training's secure internal network. Which of the following technologies would allow you to configure this port and support both requirements?

A: Implement NAC

In this scenario, implementing NAC can identify which machines are known and trusted Dion Training assets and provide them with access to the secure internal network. NAC could also determine unknown machines (assumed to be those of CompTIA employees) and provide them with direct internet access only by placing them onto a guest network or VLAN. While MAC filtering could be used to allow or deny access to the network, it cannot by itself control which set of network resources could be utilized from a single ethernet port.

Q: Which of the following IEEE specifications describes the use of network authentication?

A: 802.1x

The IEEE 802.1x standard is a network authentication protocol that opens ports for network access when an organization authenticates a user's identity and authorizes them for access to the network. This defines port security. The user's identity is determined based on their credentials or certificate, which is confirmed by the RADIUS server.

Q: Users connecting to an SSID appear to be unable to authenticate to the captive portal. Which of the following is the MOST likely cause of the issue?

A: RADIUS

Captive portals usually rely on 802.1x, and 802.1x uses RADIUS for authentication

Q: A company needs to implement stronger authentication by adding an authentication factor to its wireless system. The wireless system only supports WPA with pre-shared keys, but the backend authentication system supports EAP and TTLS. What should the network administrator implement?

A: 802.1x using EAP with MSCHAPv2

Since the backend uses a RADIUS server for back-end authentication, the network administrator can install 802.1x using EAP with MSCHAPv2 for authentication. The Extensible Authentication Protocol (EAP) is a framework in a series of protocols that allows for numerous different mechanisms of authentication, including things like simple passwords, digital certificates, and public key infrastructure. Microsoft Challenge Handshake Authentication Protocol version 2 (MS-CHAP v2) is a password-based authentication protocol that is widely used as an authentication method in PPTP-based (Point to Point Tunneling Protocol) VPNs and can be used with EAP.

Index

Severity Levels (SEA-CC-EW-NUSE-NOP-DEBUG)

Severity levels range from zero to seven, with zero being the most severe & seven being the least:

Level 0 is used for an **emergency** and is considered the **most severe condition** because the system has become unstable. REMEMBER: SE (Severe Emergency).

Level 1 is used for an **alert condition** and means that there is a condition that should be corrected immediately. REMEMBER: A (Alert).

Level 2 is used for a **critical condition**, and it means that there is a failure in the system's primary application, and it requires immediate attention. REMEMBER: CC (Critical Condition).

Level 3 is used for an **error condition**, and it means that something is happening to the system that is preventing the proper function. REMEMBER: E (Error).

Level 4 is used for **warning conditions (W)** and may indicate that an error will occur if action is not taken soon

Level 5 is used for **notice conditions** indicating **unusual events**, but they are not error conditions REMEMBER: NUSE (Notice of Unusual Event).

Level 6 is used for **information conditions** which are **normal operational (NOP) messages** & require no action

Level 7 is used for **debugging (DEBUG) conditions** and provides information useful to developers as they are debug their networks and applications

Remember the order of 0 = Most Severe & 7 = Least Severe as akin to RING 0 being the most privileged protection ring in an OS, representing the OS Kernel, or as 0 = m0st severe (hey if it looks stupid but works, it ain't stupid!) AND note that there are 8 security levels: 0 to 7, inclusive!

Persistent & Non-Persistent Agents

A non-persistent agent is used to access the device during a one-time check-in at login. A persistent agent is agent software that resides on the client making the connection, and a non-persistent agent is software the client runs (usually from a browser) as they are connecting so the agent can perform the checks, but the software does not permanently stay with the client after they disconnect. This is beneficial in BYOD (Bring Your Own Device) policies.

Index

Remediation Strategies for Embedded Industrial Control Systems (ICS)

Q: What remediation strategies are the MOST effective in reducing the risk to an embedded ICS from a network-based compromise? (Select TWO)

A: Segmentation and Disabling Unused Services (NOT Patching)

Explanation: Segmentation is the best method to reduce the risk to an embedded ICS system from a network-based compromise. By segmenting the devices off the main portion of the network, we can better protect them.

Additionally, you could disable unused services to reduce the footprint of the embedded ICS. Many of these embedded ICS systems have a large number of default services running. So, by disabling the unused services, we can better secure these devices.

A NIDS (Network Intrusion Detection System) might detect an attack or compromise, but it would not reduce the risk of the attack succeeding since it can only detect it.

<u>*Patching is difficult for embedded ICS devices since they usually rely on customized software applications that rarely provide updates.*</u>

Q: The local electric power plant contains both business networks and ICS/SCADA networks to control their equipment. Which technology should the power plant's security administrators look to implement first as part of configuring better defenses for the ICS/SCADA systems?

A: Intrusion Prevention System (IPS)

Since this question is focused on the ICS/SCADA (Supervisory Control & Data Acquisition Systems) network, the best solution would be implementing an Intrusion Prevention System. ICS/SCADA machines utilize very specific commands to control the equipment and to prevent malicious activity. You could set up strict IPS rules to prevent unknown types of actions from being allowed to occur.

Automated patch management should not be conducted, as ICS/SCADA systems must be tested before conducting any patches. Often, patches will break ICS/SCADA functionality.

Anti-virus software may or may not be able to run on the equipment as well since some ICS/SCADA systems often do not rely on standard operating systems like Windows.

Q: Syed is developing a vulnerability scanner program for a large network of sensors to monitor his company's transcontinental oil pipeline. What type of network is this?

A: SCADA

Index

SNMP Security Options / Levels

Q: You are configuring a network to utilize SNMPv3 to send information from your network devices back to an SNMP manager. Which of the following SNMP options should you enable to ensure the data is transferred confidentially?

A: authPriv:

In SNMPv3, the authPriv option ensures that the communications are sent with authentication and privacy. This uses MD5 or SHA for authentication and DES encryption for privacy.

Level	Authentication	Encryption	What Happens
noAuthNoPriv	Username	No	Uses a username match for authentication
authNoPriv	Message Digest Algorithm (MD5) or Secure Hash Algorithm (SHA)	No	Provides authentication based on Hashed Message Authentication Code (HMAC)-MD5 or HMAC-SHA algorithms.
authPriv	MD5 or SHA	Data Encryption Standard (DES)	Provides authentication based on HMAC-MD5 or HMAC-SHA. Additionally, provides DES 56-bit encryption based on the Cipher Block Chaining (CBC)-DES (DES-56) standard.

Table: SNMPv3 Security Levels. CISCO Source PDF.

SNMP Walk

SNMP Walk can be used to determine if the counter is using 32 bits or 64 bits by querying the OID of the endpoint (router interface). This is a complex topic beyond the scope of the Network+ exam (how to use the SNMP Walk tool) and usually serves as a type of in-depth question that CompTIA might ask to determine if a candidate has actual real-world experience in networking or just studied from a textbook. Some instructors like to claim that CompTIA uses these types of questions to determine if someone is cheating because only people who studied from a "brain dump" are likely to get this question correct! This type of question reminds you that it is ok not to know all the answers on test day. Just take your best guess, and then move on!

Index

SNMP Traps

An SNMP trap is a type of SNMP Protocol Data Unit (PDU). Unlike other PDU types, with an SNMP trap, an agent can send an unrequested message to the manager to notify about an important event.

The Simple Network Management Protocol (SNMP) uses ports 161 and 162, and it is a networking protocol used for the management and monitoring of network-connected devices in Internet Protocol networks. A trap is an unsolicited, asynchronous notification sent by an agent to the manager, to notify the management of a significant event that is occurring in real-time, such as an alarming condition.

A Verbose Trap may contain all the information about a given alert or event as its payload, and contains more information and data than a granular trap therefore necessitating more bandwidth for transmission.

A Granular Trap contains a *unique OID* and a value for that OID. It's sent by an agent to a manager and comprises a **single key-value pair** about a significant event or condition occurring in real-time.

Object Identifier (OID) Numbers uniquely identify managed objects in an MIB hierarchy. This can be depicted as a tree, the levels of which are assigned by different organizations. **An OID identifies a variable that can be read or set using the SNMP protocol.**

The Management Information Base (MIB) is a collection of information organized **hierarchically**, containing Object Identifiers (OIDs). There are two types of MIBs: scalar and tabular. Scalar objects define a single object instance whereas tabular objects define multiple related object instances grouped in MIB tables. MIBs are collections of definitions which define the properties of the managed object within the device to be managed.

MIB Example: The typical objects to monitor on a printer are the different cartridge states and maybe the number of printed files, and on a switch the typical objects of interest are the incoming and outgoing traffic as well as the rate of package loss or the number of packets addressed to a broadcast address.

Q: Which of the following components is used by an agent to send a complete set of key-values pairs about a significant event or condition that is occurring in real-time by providing a full list of variables and values for a given device to a manager?

A: Verbose Trap

Q: Which of the following components is used to identify a variable that may be set or read using SNMP?

A: OID

Q: A technician installs a new piece of hardware and now needs to add the device to the network management tool database. However, when adding the device to the tool using SNMP credentials, the tool cannot successfully interpret the results. Which of the following needs to be added to allow the network management tool to interpret the new device and control it using SNMP?

A: MIB

Index

Port Security AKA Persistent MAC Learning AKA Sticky MAC

Port Security, also known as persistent MAC learning or Sticky MAC, is a security feature that enables an interface to retain dynamically learned MAC addresses when the switch is restarted or if the interface goes down and is brought back online. This is a security feature that can be used to prevent someone from unplugging their office computer and connecting their laptop to the network jack without permission since the switch port connected to that network jack would only allow the computer with the original MAC address to gain connectivity.

Q: You are working as a network administrator and are worried about the possibility of an insider threat. You want to enable a security feature that would remember the Layer 2 address first connected to a particular switch port to prevent someone from unplugging a workstation from the switch port and connecting their personal laptop to it instead. Which of the following security features would BEST accomplish this goal?

A: Port Security

Q: A network administrator recently set up a network computer lab and discovered some connectivity issues. The administrator can ping the fiber uplink interface, but none of the new workstations plugged into the switch are responding to the technician's ICMP requests. Which of the following actions should the technician perform next?

A: Determine if the Link Lights are lit for the ports

Easy to confuse this for a scenario where port security is being used! But a technician can use the LEDs on the switchports to quickly monitor activity and performance for the interfaces. By determining if the link lights are lit for the ports, the administrator can verify if there is any activity on the network, if the ports are enabled, and if the Layer 1 components are working properly. Additionally, some switches have LEDs to indicate if the switchport is operating in half-duplex or full-duplex, and the speed of the link.

Index

Administration

Net Tools

Tracert (trace route) is a command-line utility used to **trace an IP packet's path** as it moves from its source to its destination. While using ping will tell you if the remote website is reachable or not, it will not tell you where the connection is broken. Tracert performs a **series of ICMP echo requests** to determine which device in the connection path is not responding appropriately. This will help to identify if the connectivity issue lies within your intranet or is a problem with the ISP's connection. It's thus a diagnostic utility that determines the route to a destination by sending Internet Control Message Protocol (ICMP) echo packets to the destination. **While 'tracert' is the Windows command, 'Traceroute' is used for Unix, Linux, and OS X.**

route: The route command is used to create, view, or modify manual entries in the network routing tables of a computer or server. **Think Static Routing.**

nslookup: The nslookup tool is used to troubleshoot DNS issues.

netstat: The netstat tool is used to display **network statistics** & active connections (NO DIAGNOSTIC). It's used to monitor incoming & outgoing connections, routing tables, port states & usage statistics on an interface.

nbtstat: Displays NetBIOS over TCP/IP **(NBT) protocol statistics**, NetBIOS name tables for both the local computer and remote computers, and the NetBIOS name cache. This command also allows a refresh of the NetBIOS name cache and the names registered with Windows Internet Name Service (WINS). Used without parameters, this command displays Help information. This command is available only if the Internet Protocol (TCP/IP) stack is installed as a component in the properties of a network adapter in Network Connections.

ping: The ping tool is used to test an end-to-end connection, but will not provide any data on the hops found in the connection.

The net use command is used to connect to, remove, and configure **connections to shared network resources** such as mapped drives and network printers. For example, "net use S: \\SERVER\DATA /persistent:yes" would map the DATA folder on the SERVER to your local S:\ drive on a Windows computer.

The PathPing command is a Windows command-line tool that is used to locate spots that have network latency & network loss between a client & destination. The advantages of PathPing over ping & traceroute are that each node is pinged via a single command & that the behavior of nodes is **studied over an extended period**, rather than the default ping sample of four messages or default traceroute single route trace.

arp: The arp command is used to view and modify the local Address Resolution Protocol (ARP) cache of a device, which contains recently resolved MAC addresses of IP hosts on the network.

telnet: The telnet command is used to open a command-line interface on a remote computer or server. Telnet operates in plain text mode and should never be used over an untrusted or public network.

A NetFlow Analyzer is used to perform monitoring, troubleshooting, inspection, interpretation, and synthesis of network traffic flow data. A NetFlow analyzer can help you quickly identify traffic patterns and the different applications/protocols in use on the network.

Index

A Terminal Emulator is used by a network administrator to make a given computer appear like an actual terminal or client computer networked to a server or mainframe.

An IP Scanner is used to monitor a network's IP address space in real-time and identify any devices connected to the network. Essentially, the tool will send a ping to every IP on the network and then creates a report of which IP addresses sent a response.

A Spectrum Analyzer is used to measure the magnitude of an input signal's frequency.

A Port Scanner is used to determine which ports and services are open and available for communication on a **target system**.

A Protocol Analyzer is used to capture, monitor, and analyze data transmitted over a communication channel.

Nmap, or Network Mapper, is a cross-platform, open-source tool used to scan IP addresses and ports on a target network, and to detect running services, applications, or operating systems on that network's clients, servers, and devices.

The tcpdump tool is a text-based packet capture and analysis tool that can capture packets and display the contents of a packet capture (pcap) file. While you may be able to identify the services, applications, or operating systems using tcpdump by analyzing the captured packets, tcpdump will not send specifically crafted packets to the devices as it is a passive reconnaissance tool.

The iPerf tool is used to create TCP and UDP data streams and measure the throughput of a given network. The iPerf tool is well suited to **test the throughput of the new switches** and its results can be used to create the new network performance baseline.

Q: Dion Training's remote office is experiencing poor network performance. You have been asked to look at the traffic patterns for the remote office and compare them to the network performance baselines. Which of the following tools should you utilize?

A: NetFlow Analyzer

Q: You are currently troubleshooting a workstation in the office and determined that it is an issue with the cabling somewhere between the workstation and the switch. You have tested the patch cable from the workstation to the wall jack and it is not faulty. You want to check the port on the switch next. Which of the following would BEST help you identify which switch port is associated with the workstation's wall jack?

A: Proper labeling!

You should always use proper labeling of your cables, wall jacks, and patch panels to make it easy to locate which switchport is associated with each portion of the cable distribution plant. Ensuring everything is properly labeled will help when you need to troubleshoot a network connection in your interior cable distribution plant.

Index

Q: Eduardo, a network technician, needs to protect IP-based servers in the network DMZ from an intruder trying to discover them. What should the network technician do to protect the DMZ from ping sweeps?

A: Block all ICMP Traffic to and from the DMZ

Ping sweeps are conducted using ICMP by default, not UDP, therefore disabling UDP on the servers will not stop a ping sweep.!

Q: Which of the following tools allows you to view and modify the layer 2 to layer 3 address bindings?

A: arp

Q: Dion Training has configured a new web server and connected it to their screened subnet. A network technician wants to ensure the server is properly hardened and that it only allows inbound HTTPS requests while blocking any HTTP requests. Which of the following tools should the technician utilize?

A: Port Scanner

A port scanner is used to determine which ports and services are open and available for communication on a target system. The port scanner will scan the server and display any open ports. If the technician finds that port 443 (HTTPS) is open and all other ports are closed, then they know the server has been properly hardened.

Index

Traffic Shaping

Traffic shaping, also known as packet shaping, is the manipulation and prioritization of network traffic to reduce the impact of heavy users or machines from affecting other users. Traffic shaping is used to optimize or guarantee performance, improve latency, or increase usable bandwidth for some kinds of packets by delaying other kinds.

Q: What is used to define how much bandwidth can be used by various protocols on the network?

A: Traffic Shaping

Event Management Tools

Q: Janet is a system administrator who is troubleshooting an issue with a DNS server. She notices that the security logs have filled up and must be cleared from the event viewer. She recalls this being a daily occurrence. Which of the following would BEST resolve this issue?

A: Install an event management tool, as this would allow an admin to clear event logs & move them from the server to a centralized database. This in turn prevents the logs from filling up on the server without having to delete them permanently from the logging environment.

Emergency Change Approval Board (ECAB)

If an urgent change to an enterprise network is required, there is an emergency change management process that can be used for approval, known as the Emergency Change Approval Board (ECAB). An ECAB can be executed extremely quickly to gain approval, while documentation can be completed after the change is made when using the emergency change management processes. Under regular circumstances, all changes to the enterprise network should be approved & documented through the normal change management processes.

Out-of-Band Management

Out-of-band (OOB) management is a method of remotely controlling and managing critical IT assets and network equipment using a secure connection through a secondary interface that is physically separate from the primary network connection.

Q: Your company has several small branch offices around the country, but you work as a network administrator at the centralized headquarters building. You need the capability of being able to remotely access any of the remote site's routers to configure them without having to fly to each location in person. Your company's CIO is worried that allowing remote access could allow an attacker to gain administrative access to the company's network devices. Which of the following is the MOST secure way to prevent this from occurring while still allowing you to access the devices remotely?

A: Create an out-of-band management network

Telnet and HTTP are not encrypted channels and should not be used for remote connections. Using a modem is also a bad security practice since these are subject to war dialing and provide slow connectivity speeds.

Index

Network Documentation & Diagrams

A physical network diagram is used to show the actual physical arrangement of the components that make up the network, including cables and hardware.

A logical network diagram is used to illustrate the flow of data across a network and is used to show how devices communicate with each other. These logical diagrams usually include the subnets, network objects and devices, routing protocols and domains, voice gateways, traffic flow, and network segments in a given network.

Wiring diagrams are used to clearly label which cables are connected to which ports. The more in-depth wiring diagrams will include a floorplan or rack diagram, so you can see how the cables are run in the physical environment.

A wireless site survey is the process of planning and designing a wireless network to provide a wireless solution that will deliver the required wireless coverage, data rates, network capacity, roaming capability, and quality of service (QoS). The site survey report will contain a floorplan of the areas surveyed with the wireless coverage areas and signal strengths notated on it. This is often referred to as a "heat map" by technicians. The technician performing the survey will document this information and use it as a tool during troubleshooting and optimization efforts concerning the wireless coverage in a specific office or building.

A network diagram is a visual representation of network architecture. It maps out the structure of a network with a variety of different symbols and line connections. **This information will be important when deploying a Storage Area Network (SAN) on the enterprise network.** A logical network diagram illustrates the flow of information through a network and shows how devices communicate with each other. It typically includes elements like subnets, network objects and devices, routing protocols and domains, voice gateways, traffic flow, and network segments.

A baseline is a process for studying the network at regular intervals to ensure that the network is working as designed. Network baselining is the act of measuring and rating the performance of a network in real-time situations. Providing a network baseline requires testing and reporting of the physical connectivity, normal network utilization, protocol usage, peak network utilization, and average throughput of the network usage.

A network audit entails collecting data, identifying threats and areas of weakness, and compiling **a formal audit report**. This report is then sent on to network administrators and other relevant parties.

Asset management is used to record and track an asset throughout its life cycle, from procurement to disposal.

A process flow diagram illustrates the arrangement of the equipment and accessories required to carry out the specific process, including its stream connections, stream flow rates and compositions, and the operating conditions.

Q: Jason is a network manager leading a project to deploy a SAN. He is working with the vendor's support technician to set up and configure the SAN on the enterprise network. To begin SAN I/O optimization, what should Jason provide to the vendor support technician?

A: Network Diagrams

Index

Q: Which of the following types of network documentation would provide a drawing of the network cabling imposed over the floorplan for an office building?

A: Physical Network Diagrams

Q: A wireless networking technician has completed an assessment of a wireless network and documented the detected signal strengths in various locations. Which of the following best describes this document?

A: Site Survey Report

Q: While monitoring the network, you notice that the network traffic to one of the servers is extremely high. Which of the following should you utilize to verify if this is a concern?

A: Network Baseline

High network traffic can be a sign of a possible attack conducted either by an insider or someone out of the network to steal relevant information. By reviewing the network baseline, you can determine if the traffic is actually high and if any network configurations are out of the baseline, causing the issue. By knowing what "normal" looks like, you can then more easily identify the abnormal.

Q: You have just replaced a faulty Ethernet cable in a patch panel. Within a few minutes, you find out that users are experiencing slow or no Internet connectivity all over the building. A broadcast storm has begun to occur. After removing the replacement cable, which of the following should you do NEXT?

A: Review labeling and logical network diagram documentation

You most likely have plugged the new cable into the wrong port on the patch panel. By reviewing the documentation and labeling, you might see the domain architecture, the strength of user connections, and the relationships in those connections, thereby making it easy to reassign the patch cables corrected. Something has likely been mislabeled, and the replacement of the patch cable was plugged into the wrong port and caused a loop.

Q: John is investigating a performance issue on a server and has begun by gathering its utilization statistics. John notices that the statistics are outside of the normal, acceptable ranges. What should John do next?

A: Conduct a baseline review, which is strange because the question already states that it's "outside normal, acceptable ranges" indicating that the baseline has been verified already but whatever.

Virtual Local Area Networks (VLANs)

A Virtual Local Area Network (VLAN) is a type of **network segmentation** wherein a local area network (a broadcast domain) is partitioned and isolated in a computer network **at the Data Link Layer (OSI Layer2).** VLANs are configured such that your network switches **prevent communications between different VLANs without using a router.** This allows two virtually separated networks to exist on one physical network and separates the two virtual network's data.

VLANs need a properly configured Access Control List (ACL): Without a properly configured ACL, there is no additional security provided by a VLAN. This allows network administrators the opportunity to allow or deny traffic into or out of a given VLAN for additional security via the ACL.

Q: You are working as a network administrator for Dion Training. The company has decided to allow employees to connect their devices to the corporate wireless network under a new BYOD policy. You have been asked to separate the corporate network into an administrative network (for corporate-owned devices) and an untrusted network (for employee-owned devices). Which of the following technologies should you implement to achieve this goal?

A: VLAN

Q: Which of the following must be added to a VLAN's gateway to improve the security of the VLAN?

A: ACL

802.1q

IEEE 802.1q, often referred to as **Dot1q**, is the networking standard that supports Virtual Local Area Networking (VLANs) on an IEEE 802.3 Ethernet network. The standard defines a system of **VLAN Tagging for Ethernet frames** and the accompanying procedures to be used by bridges and switches in handling such frames. The standard also contains provisions for a quality-of-service prioritization scheme commonly known as IEEE 802.1p and defines the Generic Attribute Registration Protocol.

802.1q Trunking

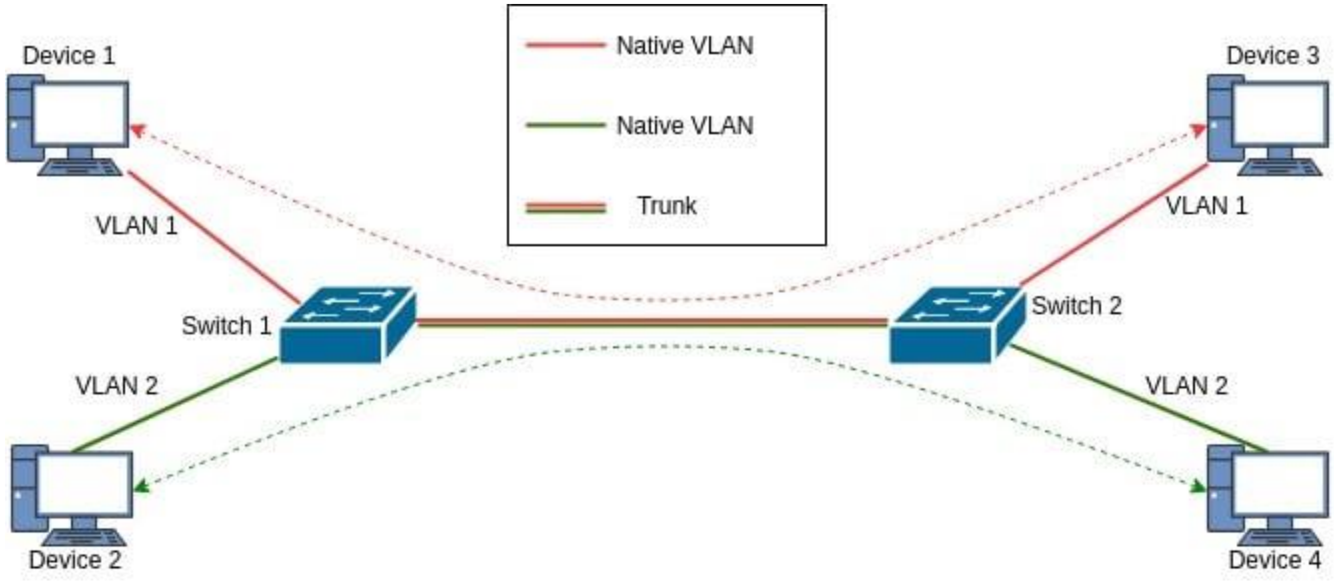
Firstly, trunking pertains to the use of VLANs.

A VLAN, as elaborated earlier, is any LAN (broadcast domain) that’s partitioned and isolated in a computer network at the Data Link Layer (OSI Layer2), and necessitates the use of a router for traffic between VLANs.

Now WTR Trunking, as networks & data centers get more complex and the number of interconnected services increases, it becomes more complex and expensive to provide dedicated cabling and network switch ports to allow for all the required connections. **VLAN trunking then, allows for multiple virtual network connections to be maintained on a small number of physical adapters**. Each Virtual Local Area Network (VLAN) gets a **unique VLAN Tag**, and each packet on the network gets branded with the tag of the VLAN it’s associated with. Network devices then **only interact with packets that have the correct tags**. This allows multiple different logical networks to run on the same cable and switch infrastructure.

Index

However, a typical Ethernet frame does not provide a field specifying which VLAN a frame belongs to, so a switch on receiving a frame would not know what VLAN to send it to. As a result, we need another protocol to help out here and so if you want to route traffic of multiple VLANs on the same switches, we'll have to use a **trunk**. A trunk connection is, simply said, nothing more but a normal link that's able to pass the traffic of multiple VLANs while maintaining separation based on VLANs. Here's an example:



Q: A workstation is connected to the network and receives an APIPA address but cannot reach the VLAN gateway of 10.10.100.254. Other PCs in the VLAN subnet can communicate with the VLAN gateway and access websites on the Internet. Which of the following is the MOST likely the source of this connectivity problem?

A: The Switch port is configured for 802.1q Trunking!

If the switchport is configured for 802.1q trunking instead of as an access host port, the workstation will be unable to reach the DHCP server through the switch and will instead fall back to using an APIPA address. APIPA is configured by default on client and server devices, not on the switch. So if it's falling back to an APIPA address, it means it could not reach the DHCP Server via the Switch.

Small Form-factor Pluggable (SFP) transceivers are used on routers as hot-pluggable network interface modules, they are NOT used on workstations!

A workstation's OS update status is unlikely to cause the network connectivity issue, but a network interface driver change might.

Therefore, the most likely cause of this issue is that the switchport was configured as a trunking port instead of an access port.

Index

Q: An administrator has configured a new 250 Mbps WAN circuit, but a bandwidth speed test shows poor performance when downloading larger files. The download initially reaches close to 250 Mbps but begins to drop and show spikes in the download speeds over time. The administrator checks the interface on the router and sees the following:

DIONRTR01# show interface eth 1/1 GigabitEthernet 1/1 is up, line is up Hardware is GigabitEthernet, address is 000F.33CC.F13A Configured speed auto, actual 1Gbit, configured duplex fdx, actual fdx Member of L2 VLAN 1, port is untagged, port state is forwarding.

Which of the following actions should be taken to improve the network performance for this WAN connection?

A: Assign the interface an 802.1q tag to its own VLAN

Explanation:

- ***The WAN interface (eth 1/1) is currently untagged and is being assigned to the default VLAN (VLAN 1)***

- ***If there are numerous devices in the default VLAN, the VLAN may be overloaded or oversubscribed leading to a reduction in the network performance***

- ***To solve this issue, you would assign the WAN interface to a VLAN with less traffic or to its own VLAN***

- ***By adding an 802.1q tag (VLAN tag) to the interface, you can assign it to its own individual VLAN and eliminate potential overloading or oversubscription issues***

Other (Incorrect) Options:

1. ***The interface is already set to full-duplex (fdx) and is operating in full-duplex (fdx). Therefore, the issue is not a duplexing mismatch.***

2. ***The configuration shows that the interface is already using a GigabitEthernet, so you do not need to replace the transceiver with a 1000Base–T module. Also, the physical layer is working properly, and a link is established, as shown by the output "GigabitEthernet 1/1 is up", showing the current transceiver is functioning properly at 1 Gbps.***

3. ***Lastly, while issuing the shutdown command and then re-enabling the interface could clear any errors, based on the interface status shown we have no indications that errors are being detected or reported.***

Index

Q: A technician is configuring a computer lab for the students at Dion Training. The computers need to be able to communicate with each other on the internal network, but students using computers should not be able to access the Internet. The current network architecture is segmented using a triple-homed firewall to create the following zones:

ZONE INTERFACE, IP address -------------------------------------- PUBLIC, eth0,

66.13.24.16/30 INSTRUCTORS, eth1,

172.16.1.1/24 STUDENTS, eth2,

192.168.1.1/24

What rule on the firewall should the technician configure to prevent students from accessing the Internet?

A: Deny all traffic from eth2 to eth0

By denying all traffic from the eth2 to eth0, you will block network traffic from the internal (STUDENT) network to the external (PUBLIC) network over the WAN connection. This will prevent the students from accessing the Internet by blocking all requests to the Internet. For additional security, it would be a good idea to also block all traffic from eth0 to eth2 so that inbound traffic from the internet cannot communicate with the student's computers. But, since the outbound connections from the students to the internet are being blocked, the student will be unable to access any webpages since they cannot send a request over port 80 or 443. Additionally, by choosing this rule, we have not blocked any network traffic between the instructors and the students.

Q: A network technician is asked to redesign an Ethernet network before some new monitoring software is added to each network's workstation. The new software will broadcast statistics from each host to a monitoring server for each of the company's five departments. The added network traffic is a concern of management that must be addressed. How should the technician design the new network?

A: Place each department in a separate VLAN to increase broadcast domains

Each VLAN becomes its own broadcast domain, and this would minimize the total number of broadcast messages sent to every client on the network. For traffic to enter or leave a VLAN, it must go through a router or a layer 3 switch. A collision domain will not prevent a broadcast message from being sent. Increasing the number of switches will not reduce or increase the number of broadcast messages. To minimize the number of broadcast messages, you need to increase the number of broadcast domains.

Q: You are setting up uplink ports for multiple switches to communicate with one another. All of the VLANs should communicate from the designated server switch. Which of the following should be set on the trunk ports if VLAN 1 is not the management VLAN?

A: Port Tagging

The 801.q standard is used to define VLAN tagging (or port tagging) for Ethernet frames and the accompanying procedures to be used by bridges and switches in handling such frames. Traffic should be properly tagged when combined over a single trunk port to ensure they are not sent to the wrong VLAN by mistake. If VLAN tagging is not enabled, all of the VLAN traffic will be sent to the native or default VLAN, VLAN 1. By default, VLAN 1 is enabled, and all unused ports are assigned to it.

Q: An attacker has configured their machine to report itself as a switch when connected to a wired network in an attempt to exploit your enterprise network. Which of the following types of attacks is being conducted?

A: VLAN Hopping

Q: Which of the following describes the ID of a specified native VLAN when traffic passes over a trunk?

A: It becomes the default VLAN for untagged frames

Trunk ports carry all traffic, regardless of VLAN number, between all switches in a LAN. The VLAN designation for a trunk port is its native or default VLAN. If the trunk port has a native VLAN that differs from the tag placed on the frame as it entered the access port, the switch leaves the tag on the frame and sends the tagged frame along to the next switch or switches. If the trunk port's native VLAN is the same as the access port's VLAN, then the switch drops the tag and sends the untagged frame out of the trunk port.

VLAN Trunking Protocol (VTP)

VLAN Trunking Protocol (VTP) is a Cisco proprietary protocol that propagates the definition of Virtual Local Area Networks (VLAN) on the whole local area network. To do this, VTP carries VLAN information to all the switches in a VTP domain. VTP advertisements can be sent over 802.1Q, & ISL trunks. In other words, it allows a VLAN created on one switch to be propagated to other switches in a group of switches in a VTP domain.

Q: Which of the following protocols must be implemented for two switches to share VLAN information?

A: VTP

Index

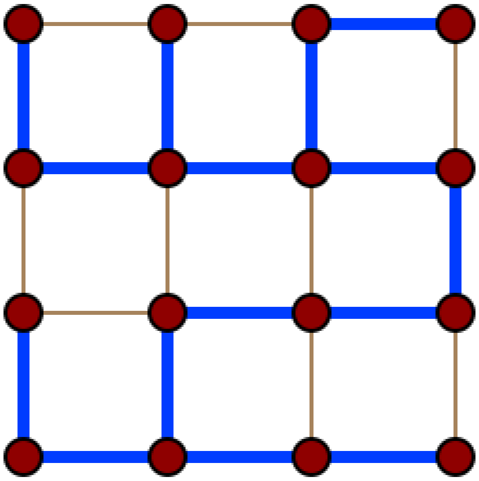
Spanning Tree Protocol (STP) – 802.1d

The Spanning Tree Protocol (STP) is a network protocol that builds a loop-free logical topology (*topology*: arrangement of elements in a computer network) for Ethernet networks **to prevent bridge loops and the broadcast storms that result from them**. Spanning tree also allows a network design to include backup links providing fault tolerance if an active link fails.

As the name suggests, STP creates a spanning tree that characterizes the relationship of nodes within a network of connected layer-2 bridges, and disables those links that are not part of the spanning tree, leaving a single active path between any two network nodes. STP is based on an algorithm that was invented by Radia Perlman while she was working for Digital Equipment Corporation.

In 2001, the IEEE introduced Rapid Spanning Tree Protocol (RSTP) as 802.1w. RSTP provides significantly faster recovery in response to network changes or failures, introducing new convergence behaviors and bridge port roles to do this. RSTP was designed to be backwards-compatible with standard STP.

STP was originally standardized as IEEE 802.1d but the functionality of Spanning Tree (**802.1d**), Rapid Spanning Tree (**802.1w**), and Multiple Spanning Tree (**802.1s**) has since been incorporated into IEEE 802.1Q-2014.



Spanning Trees: In graph theory, a spanning tree *T* of an undirected graph *G,* is a subgraph that is a tree which includes all of the vertices of G. In general, a graph may have several spanning trees, but a graph that is not connected will not contain a spanning tree. If all of the edges of *G* are also edges of a spanning tree *T* of *G*, then *G* is a tree and is identical to *T* (that is, a tree has a unique spanning tree, and it is itself).

A tree itself is a connected undirected graph with no cycles.

Several pathfinding algorithms, including Dijkstra's algorithm and the A* search algorithm, internally build a spanning tree as an intermediate step in solving the problem.

Broadcast Storms/Radiation and Chernobyl Packets

A **Broadcast Storm or Broadcast Radiation** is the accumulation of broadcast and multicast traffic on a computer network. Extreme amounts of broadcast traffic constitute a "broadcast storm". It can consume sufficient network resources so as to render the network unable to transport normal traffic. A packet that induces such a storm is occasionally nicknamed a **Chernobyl packet**!

Index

Switching Loops

A **Switching Loop or Bridge Loop** occurs in computer networks when there is more than one layer-2 path between two endpoints (e.g. multiple connections between two network switches or two ports on the same switch that are connected to each other). The loop creates broadcast storms as broadcasts and multicasts are forwarded by switches out every port, the switch or switches will repeatedly rebroadcast the same broadcast messages thus flooding the network. Since the layer-2 header does not include a Time To Live (TTL) field, if a frame is sent into a looped topology, it can loop forever.

While a physical topology that contains switching or bridge loops is attractive for redundancy reasons, yet a switched network must not have loops. The solution is to allow physical loops, but to create a loop-free logical topology using link aggregation, shortest path bridging, spanning tree protocol or TRILL on the network switches.

Q: A technician installs three new switches to a company's infrastructure. The network technician notices that all the switchport lights at the front of each switch flash rapidly when powered on and connected. After about a minute, the switches return to normal operation. Additionally, there are rapidly flashing amber lights on the switches when they started up the next day. What is happening to the switches?

A: The switches are running through their spanning tree process

The switch port lights flashing is indicating that the switch is performing the spanning tree process. The Spanning Tree Protocol (STP) is responsible for identifying links in the network and shutting down the redundant ones, preventing possible network loops. To do so, all switches in the network exchange Bridge Protocol Data Units (BPDUs – frames that contain information about STP) between them to agree upon the root bridge. When spanning tree protocol is enabled on a switch, the switchports will go through five port states: blocking, listening, learning, forwarding, and disabled to create a loop-free switching environment.

Q: Sahra connects a pair of switches using redundant links. When she checks the link status of the two ports, one of them is not active. She changes the inactive link to another switchport, but the second link still remains inactive. What MOST likely is causing the second link to become disabled?

A: Spanning Tree

The basic function of STP is to prevent bridge loops and the resulting broadcast radiation. If STP detects a switching loop being created by the redundant connection, it will disable the switchport automatically.

Q: A 48-port switch on the Dion Training network just rebooted and all the clients are attempting to obtain a new DHCP address. Which of the following issues may begin to occur?

A: Broadcast Storm

The DHCP discover, offer, request, and acknowledge process occurs using broadcast messages, therefore a broadcast storm could occur due to all 48 clients attempting to receive a DHCP assignment simultaneously.

Index

Spanning Tree Protocol States

The spanning tree protocol supports four different states on any given switchport:

1. The switchport will go into a **Blocking** state when it receives a BPDU that indicates there is a better path to the root bridge and the switchport itself is not a root port or designated port. If the switchport is a root port or designated port, it will then move to a listening state.
2. During the **Listening** state, the switchport will discard any frames it receives.
3. When the switchport is in a **Learning** state, it will listen for and process BPDUs it receives and update its MAC address table. During a listening state, the switchport will not forward any of the frames to others.
4. A switchport in a **Forwarding** state will process BPDUs, update its MAC table, and forward the BPDUs to other switchports. This process will ensure that switching loops are prevented in a network.

Q: What state is the switchport with the LEAST desirable path placed by the spanning tree protocol when a switch has multiple paths to reach the root bridge?

A: Blocking

Q: A network technician wants to centrally manage the switches and segment the switches into separate broadcast domains. The Dion Training network is currently using VLAN 1 for all of its devices and uses a single private IP address range with a 24-bit mask. Their supervisor wants VLAN 100 to be the management subnet and all of the switches must share VLAN information. Which of the following should the technician configure to meet these requirements?

A: Configure VTP (NOT STP!) and 802.1q on the inter-switch connections with native VLAN 100 and Configure VLSM for the IP address range

Q: After installing some new switches in your network, you notice that a switching loop has begun to occur. You contact the manufacturer's technical support for your switches, and they recommended that you enable 802.1d. Which of the following BEST represents why the manufacturer suggested this?

A: STP uses BPDUs (NOT Split Horizon!) to detect loops in network topologies

Index

Storage & Jumbo Frames

Jumbo frames are Ethernet frames whose MTU (Maximum Transmission Unit) is greater than 1500 Bytes. To increase performance, you should use jumbo frames only when you have a dedicated network or VLAN, and you can configure an MTU of 9000 on all equipment. Because of this, jumbo frames are most commonly used in Storage Area Networks (SAN), but apparently not when using a Network Attached Storage (NAS).

A Network-Attached Storage (NAS) device is a self-contained computer that connects to a home or business network and can share files over TCP/IP. It is a rapidly growing choice for data storage and can provide data access to numerous users on a network. A NAS consists of a hard disk for storage of files and usually utilizes a RAID system for redundancy and/or performance.

iSCSI (pronounced "i-scuzzy") is used to facilitate data transfers over intranets and to manage storage over long distances. It can be used to transmit data over local area networks (LANs), wide area networks (WANs), or the Internet and can enable location-independent data storage and retrieval.

Q: You work for a small company that wants to add a shared drive to their network. They are looking for a simple solution that will easily integrate into the existing network, be easy to configure, and share files with all network clients over TCP/IP. Which of the following is the BEST recommended storage for this network?

A: NAS

CLI Commands for CISCO Networking Devices

show config: The "show configuration" command is used to display the device's current configuration. This would show whether or not the DHCP snooping was enabled on this device.

show interface: The "show interface" command is used to display the statistics for a given network interface.

show diagnostic: The "show diagnostic" command is used to display details about the hardware and software on each node in a networked device.

show route: The "show route" command is used to display the current state of the routing table for a given network device.

Q: You just started work as a network technician at Dion Training. You have been asked to determine if Ethernet0/0 is currently connected using OSPF or EIGRP on one of the network devices. Which of the following commands should you enter within the command line interface?

A: show route

To determine if Ethernet0/0 is connected using OSPF or EIGRP, you would need to use the "show route" command to display the current status.

Index

Autonomous Systems (AS)

An Autonomous System (AS) is a collection of connected Internet Protocol (IP) routing prefixes under the control of one or more network operators on behalf of a **single administrative entity or domain**, that presents a common and clearly defined routing policy to the Internet. **Each AS is assigned an Autonomous System Number (ASN), for use in Border Gateway Protocol (BGP) routing.** Autonomous System Numbers are assigned to Local Internet Registries (LIRs) and end user organizations by their respective Regional Internet Registries (RIRs), which in turn receive blocks of ASNs for reassignment from the **Internet Assigned Numbers Authority (IANA)**. The IANA also maintains a registry of ASNs which are reserved for private use (and should therefore not be announced to the global Internet).

The Border Gateway Protocol (BGP) is an exterior gateway protocol that's used for routing between autonomous systems

Q: Routing prefixes are assigned in blocks by IANA and distributed by the Regional Internet Registry (RIR). What are these known as?

A: Autonomous System Number

High-Availability via BGP

Q: Your company wants to create highly available datacenters. Which of the following will allow the company to continue maintaining an Internet presence at all sites if the WAN connection at their own site goes down?

A: BGP

If a WAN link goes down, BGP will route data through another WAN link if redundant WAN links are available. Border Gateway Protocol (BGP) is a standardized exterior gateway protocol designed to exchange routing and reachability information between Autonomous Systems (AS) on the Internet. The protocol is often classified as a path vector protocol but is sometimes also classed as a distance-vector routing protocol.

A load balancer would work at one site, but would not allow routing of the WAN connections at all the other sites since they are autonomous systems and BGP is used to route traffic between autonomous systems.

Index

Link Aggregation & the Link Aggregation Control Protocol (LACP) – 802.3ad

In computer networking, link aggregation is the combining (aggregating) of multiple network connections in parallel by any of several methods. Link aggregation increases total throughput beyond what a single connection could sustain, and provides redundancy where all but one of the physical links may fail without losing connectivity. A Link Aggregation Group (LAG) is the combined collection of physical ports.

Other umbrella terms used to describe the concept include trunking, bundling, bonding, channeling, or teaming.

Implementation may follow vendor-independent standards such as Link Aggregation Control Protocol (LACP) for Ethernet, **defined in IEEE 802.1AX or the previous IEEE 802.3ad**, but also proprietary protocols.

Motivation:

Link aggregation increases the bandwidth and resilience of Ethernet connections.

Bandwidth requirements do not scale linearly. Ethernet bandwidths historically have increased tenfold each generation: 10 megabit/s, 100 Mbit/s, 1000 Mbit/s, 10,000 Mbit/s**. If one started to bump into bandwidth ceilings, then the only option was to move to the next generation, which could be cost prohibitive.** An alternative solution, introduced by many of the network manufacturers in the early 1990s, is to use link aggregation to combine two physical Ethernet links into one logical link. Most of these early solutions required manual configuration and identical equipment on both sides of the connection

There are three single points of failure inherent to a typical port-cable-port connection, in either a computer-to-switch or a switch-to-switch configuration: the cable itself or either of the ports the cable is plugged into can fail. Multiple **logical** connections can be made, but many of the higher-level protocols were not designed to fail over completely seamlessly. Combining multiple **physical** connections into one logical connection using link aggregation provides more resilient communications.

Link Aggregation Control Protocol

Within the IEEE Ethernet standards, the Link Aggregation Control Protocol (LACP) provides a method to control the bundling of several physical links together to form a single logical link. LACP allows a network device to negotiate an automatic bundling of links by sending LACP packets to their peer, a directly connected device that also implements LACP. LACP Features and practical examples:

1. Maximum number of bundled ports allowed in the port channel: Valid values are usually from 1 to 8.
2. LACP packets are sent with multicast group MAC address 01:80:C2:00:00:02
3. During LACP detection period
    a. LACP packets are transmitted every second
    b. Keep-alive mechanism for link member: (default: slow = 30s, fast=1s)
4. Selectable load-balancing mode is available in some implementations
5. LACP mode :
    a. Active: Enables LACP unconditionally.
    b. Passive: Enables LACP only when an LACP device is detected. (This is the default state)

Index

Advantages over static configuration:

Failover occurs automatically: When a link has an intermediate failure, for example in a media converter between the devices, a peer system may not perceive any connectivity problems. With static link aggregation, the peer would continue sending traffic down the link causing the connection to fail.

Dynamic configuration: The device can confirm that the configuration at the other end can handle link aggregation. With static link aggregation, a cabling or configuration mistake could go undetected and cause undesirable network behavior.

Practical notes

LACP works by sending frames aka data units (LACPDUs) down all links that have the protocol enabled. If it finds a device on the other end of a link that also has LACP enabled, that device will independently send frames along the same links in the opposite direction enabling the two units to detect multiple links between themselves and then combine them into a single logical link. LACP can be configured in one of two modes: active or passive. In active mode, LACPDUs are sent 1 per second along the configured links. In passive mode, LACPDUs are not sent until one is received from the other side, a speak-when-spoken-to protocol.

Q: The network administrator is troubleshooting the switchports for a file server with dual NICs. The file server needs to be configured for redundancy, and the dual NICs need to be combined for maximum throughput. What feature on the switch should the network administrator ensure is enabled for best results?

A: LACP (think about aggregation whenever the question pertains to combining the bandwidth of multiple links!)

Q: Dion Training has begun to notice slow response times from their internal network file server to workstations on their local area network. After adding several new employees and workstations, the network administrator determined that the server is experiencing requests for up to 2 Gbps of simultaneous data transfer which has resulted in congestion at the server's NIC. Which of the following actions should the network administrator implement to remove this performance bottleneck?

A: Install a NIC, implement NIC teaming and configure 802.3ad

Since the bottleneck has been identified as the server's NIC card, a second network interface card (NIC) should be installed, NIC teaming should be implemented, and 802.3ad (LACP) should be configured on the switch. NIC teaming allows a server to load balance any data sent or received across two network interface cards, effectively doubling the server's network throughput. The switch should be configured to support LACP to support the NIC teaming on the server.

Index

Remote Access Issues on the LAN w/ Hostnames

Q: Michael, a system administrator, is troubleshooting an issue remotely accessing a new Windows server on the local area network using its hostname. He cannot remotely access the new server, but he can access another Windows server using its hostname on the same subnet. Which of the following commands should he enter on his workstation to resolve this connectivity issue?

A: C:\windows\system32> nbtstat -R

<u>Since this is a Windows-based network, the client is likely attempting to connect to the servers using NetBIOS. NetBIOS stores a local cached name table in the LMHOSTS file on each client.</u> If the entry in the client file is pointing to the wrong IP, this could cause the connectivity issues described. Therefore, the sysadmin should enter the "nbtstat -R" command to purge and reload the cached name table from the LMHOST file on their Windows workstation.

What is NetBIOS?

NetBIOS (Network Basic Input/Output System) is a network service that **enables applications on different computers to communicate** with each other across a Local Area Network (LAN). It was developed in the 1980s for use on early, IBM-developed PC networks. A few years later, Microsoft adopted NetBIOS and it became a de-facto industry standard. Currently, NetBIOS is mostly relegated to specific legacy application use cases that still rely on this suite of communication services.

NetBIOS by itself is not a network protocol, as it does not provide a standard frame or data format for transmission. Thus original NetBIOS iterations used a standard frame format that was provided by the NetBIOS Extended User Interface (NetBEUI) protocol and later revisions used the IPX (Internetwork Packet Exchange)/SPX (Sequenced Packet Exchange) and TCP/IP (Transmission Control Protocol/Internet Protocol) protocols, a combination which is referred to as NetBIOS over TCP/IP (NBT). NBT may still be in use on enterprise networks. <u>NetBIOS for Microsoft Operating Systems is only supported on IPv4 networks and is not compatible with the newer IPv6 protocol stack.</u>

Q: Damaris is troubleshooting a WINS-connectivity issue on a Windows server. She wants to find out the name of the server she is working on. Which of the following commands should she utilize to display the NetBIOS name of the server?

A: hostname

The hostname command is used to view or change a computer's hostname and domain. <u>On a Windows system, the hostname, computer name, and NetBIOS name are all the same.</u>

Index

Cloud Terminology

Measured Service is a term that IT professionals apply to cloud computing that references services where the cloud provider measures or monitors the provision of services for various reasons, including billing, effective use of resources, or overall predictive planning.

Rapid Elasticity is used to describe scalable provisioning or the capability to provide scalable cloud computing services.

- Rapid elasticity is very critical to meet the fluctuating demands of cloud users.
- The downside of rapid elasticity implementations is that they can cause significant loading of the system due to the high number of resource allocation and deallocation requests.
- Rapid elasticity can also be a security threat to your organization's data due to data remanences.

On-demand refers to the fact that a consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service provider.

Resource Pooling refers to the concept that allows a virtual environment to allocate memory and processing capacity for use by virtual machines.

'Desktop as a Service' - DaaS in this exam seems to refer to 'Desktop as a Service', which are Virtualized Desktop Infrastructure (VDI) services.

Community Cloud in computing is a collaborative effort in which infrastructure is shared between several organizations from a specific community with common concerns, whether managed internally or by a third party and hosted internally or externally.

- Community Cloud is a hybrid form of private cloud: they are multi-tenant platforms that enable different organizations to work on a shared platform.
- Community Cloud may be hosted in a data center, owned by one of the tenants, or by a third-party cloud services provider and can be either on-site or off-site.

High Availability (HA) is a component of a technology system that eliminates single points of failure to ensure continuous operations or uptime for an extended period.

Index

Thin Clients

  - ▪ A Thin Client is a stateless, fanless desktop terminal that has no hard drive.

- All features typically found on the desktop PC, including applications, sensitive data, memory, etc., are stored back in the data center when using a thin client, most typically in a VDI or other environment.

- To set up a thin client, you will first connect it to the network, update its security software, and then install/configure any applications needed to access the VDI environment.

VM Network Types

<u>Internal</u>, each VM can communicate between the host and the other VMs.

<u>External</u>, the VMs would have internet access.

<u>Private</u> network connection type will create a switch that is usable only by the VMs. The VMs cannot use the switch to communicate with the host.

<u>Localhost</u>, each VM could only communicate with itself.

Type I & Type II Hypervisors

<u>Type 2 Hypervisor</u>: Runs on top of an existing operating system.

<u>Type 1 Hypervisor:</u> Also known as bare metal, uses a **specialized hypervisor OS** to run the virtual machines (**such as VMWare's ESXi**).

  - ▪ Also known as a virtual machine monitor, is a process that creates and runs virtual machines (VMs).

- A hypervisor allows one host computer to support multiple guest VMs by virtually sharing its resources, like memory and processing.

  - ▪ To create and provision virtual machines within the Windows 2019 operating system, you can use a Type II Hypervisor like VMWare or VirtualBox.

Virtualization Tech on Intel is called VT and on AMD it's AMD-V

Q: When using a Type 1 hypervisor virtualized environment, which of the following hardware types is necessary to connect the VMs to the corporate network?

A: Virtual NIC

A VM includes a virtual NIC: a type of virtual adapter that can be configured on logical partitions to provide a network interface. This vNIC can be paired & mapped to a physical NIC to get the VM onto the network.

Index

Q: You are configuring a new machine with a hypervisor and several operating systems hosted within it to develop some new applications. You want to ensure that the hypervisor's various virtual machines can communicate with each other over a network, but you don't want this network traffic to leave the hypervisor itself. What is the BEST solution to meet these requirements?

A: Install and configure a virtual switch

A virtual switch (vSwitch) is a software program that allows one virtual machine (VM) to communicate with another. A virtual switch is a software application that allows communication between virtual machines. A vSwitch does more than just forward data packets, it intelligently directs the communication on a network by checking data packets before moving them to a destination. This is usually created within the hypervisor's software.

Top-Talkers & Top-Listeners

Top Talkers are the computers that send the most data, either from your network or into your network.

Top Listeners are the hosts that receive most of the data, streaming or downloading large amounts of data from the internet. These computers can create heavy traffic and lower performance.

Datacenter Sites

A warm site is a type of facility an organization uses to recover its technology infrastructure when its primary data center goes down. A warm site features an equipped data center but no customer data.

A cold site is a backup facility with little or no hardware equipment installed. A cold site is essentially an office space with basic utilities such as power, cooling system, air conditioning, and communication equipment, etc.

A hot site is a real-time replication of an existing network environment. All data generated and stored at the primary site is immediately replicated and backed up at the disaster recovery site.

A cloud site is a virtual recovery site that allows you to create a recovery version of your organization’s enterprise network in the cloud. Cloud sites are useful when your disaster recovery plan includes migrating to a telework or remote operations environment.

Q: Which of the following type of sites might contain a datacenter with equipment, but it is not configured and doesn't contain any user or customer data yet?

A: Warm Site

Q: Which of the following type of sites would contain little to no hardware and could take days or weeks to become ready for use during a disaster?

A: Cold Site

Index

Datacenter Traffic Flow

North-South traffic or communication refers to traffic that enters or leaves the data center from a system physically residing outside the datacenter. North-traffic is traffic exiting the datacenter. South-traffic is traffic entering the data center.

Kind of super annoying, because you'd think traffic enters from the North and exits down South, but no, of course it's the opposite. In that case, just remember "take it up the bum" or "fire in the hole"!

Software Defined Networking

Software-defined networking (SDN) technology is an approach to network management that enables dynamic, programmatically efficient network configuration in order to improve network performance and monitoring, making it more like cloud computing than traditional network management. SDN is meant to address the static architecture of traditional networks.

SDN Layers:

The **Application Layer** focuses on the communication of resource requests or information about the network.

The **Control Layer** uses the information from applications to decide how to route a data packet on the network and to make decisions about how traffic should be prioritized, secured, and where it should be forwarded to.

The Control Plane Policing (CPP) feature allows users to configure a QoS filter that manages the traffic flow of control plane packets to protect the control plane of ***Cisco IOS (Internetworking Operating System)*** *routers and switches against reconnaissance & DoS attacks. This helps to protect the control plane while maintaining packet forwarding and protocol states despite an attack or heavy traffic load on the router or switch.*

The **Infrastructure Layer** contains the physical networking devices that receive information from the control layer about where to move the data and then perform those movements.

The **Management Plane** is used to monitor traffic conditions, the status of the network, and allows network administrators to oversee the network and gain insight into its operations.

Q: Which of the following layers within software-defined networking focuses on resource requests or information about the network?

A: Application Layer

Q: Which of the following security features should be enabled to configure a quality-of-service filter to manage the traffic flow of a Cisco router or switch and protect it against a denial-of-service attack?

A: Control Plane Policing

Index

Data Center Network Architectures: Two & Three-Tiered Archs

Traditional data center networks utilized a three-tier design that consists of a core, distribution, and access layer of switches.

- The Core Layer is considered the backbone of our network and is used to merge geographically separated networks back into one logical and cohesive unit. In general, you will have at least two routers at the core level, operating in a redundant configuration. Core switches are usually large modular chassis with very high throughput and advanced routing capabilities.
- The Distribution or Aggregation Layer is located under the core layer, and it provides boundary definition by implementing access lists and filters to define the policies for the network at large. Distribution layer switches are mid-tier speed switches with an emphasis on uplink speeds. Services, such as load balancing or firewalls, can often be found at this layer.
- The Access or Edge Layer is located beneath the distribution or aggregation layer and is used to connect all the endpoint devices like computers, laptops, servers, printers, wireless access points, and others. Access switches are the traditional top-of-rack (TOR) switch that regularly consists of 24 to 48 ports of 1 or 10Gbps speeds with similarly sized uplinks.

What are two-tier data center networks?

In the modern data center, two-tier spine and leaf architectures may be recommended, also known as Folded-CLOS. This approach is better suited to meeting the needs of modern applications, such as high-throughput and low-latency.

- Spine switches are very high-throughput, low-latency and port-dense switches that have direct high-speed (40-400Gbps) connections to each leaf switch.
- A leaf switch is typically used as a TOR switch. Leaf switches are very similar to traditional TOR switches in that they are often 24 or 48 port 1, 10 or 40Gbps access layer connections. However, they have the increased capability of either 40, 100 or 400Gbps uplinks to each spine switch.

Q: Which of the following layers is NOT used in a three-tiered data center network architecture?

A: Control Layer

Clos Network

In the field of telecommunications, a Clos network is a kind of multistage circuit-switching network which represents a theoretical idealization of practical, multistage switching systems. It was invented by Edson Erwin in 1938 and first formalized by Charles Clos. Clos networks have three stages: the ingress stage, the middle stage, and the egress stage. Each stage is made up of a number of crossbar switches, often just called *crossbars*. In electronics and telecommunications, a crossbar switch (cross-point switch, matrix switch) is a collection of switches arranged in a matrix configuration. Originally, a crossbar switch consisted literally of crossing metal bars that provided the input and output paths. Later implementations achieved the same switching topology in solid-state electronics. The crossbar switch is one of the principal telephone exchange architectures, together with a rotary switch, memory switch, and a crossover switch.

A folded-Clos (fat-tree) network is the **one-sided version of the Clos network**

Index

IP Address Deepdive

Types

Static IP Address is used when the DHCP server is disabled & clients are configured manually to join the network properly.

Automatic Private IP Addressing (APIPA) is a feature of Windows-based operating systems that enables a computer to automatically assign itself (self-configure) an IP address and subnet mask when there is no Dynamic Host Configuration Protocol (DHCP) server available to perform that function.

- When a host uses an APIPA address, it can communicate with other hosts on the same network using APIPA, but it cannot reach other networks or communicate with hosts who have managed to obtain a valid DHCP lease.
- Any address from 169.254.1.0 to 169.254.254.255 is considered an APIPA address.

Link-Local Address are also known as APIPA addresses, but apparently is the IPv6 variant

Private IP Address is an IP address reserved for internal use behind a router or other Network Address Translation (NAT) devices, apart from the public. Private IP addresses provide an entirely separate set of addresses that still allow access to a network without taking up a public IP address space**. Private IP Addresses are in the range of 10.x.x.x, 172.16-31.x.x, or 192.168.x.x.**

Localhost & Loopback IP is 127.0.0.1

Public IP Addresses - All others are considered Public IP Addresses.

Classless IP Addressing solutions allow for the use of subnets that are smaller than the classful subnets associated with Class A, Class B, or Class C networks.

Q: Andy is a network technician who is preparing to configure a company's network. He has installed a firewall to segment his network into an internal network, a DMZ or screen subnet, and an external network. No hosts on the internal network should be directly accessible by their IP address from the Internet, but they should be able to reach remote networks if they have been assigned an IP address within the network. Which of the following IP addressing solutions would work for this particular network configuration?

A: Private

Loopback Addresses

  - Loopback is the routing of signals or data streams back to their source without processing or modification, and is used primarily as a means of testing communications infrastructure.
  - **In IPv6 the Loopback Address is ::1. In IPv4, the loopback address is 127.0.0.1.**
- If there is no communication of the return packet, this indicates the network card is faulty, the cable/loopback is loose, or there is bad wiring of the loopback plug.

Index

IPv6 Address (vs IPv4 & MAC Addresses) and SLAAC & Teredo

IPv6 Addresses are written as a series of up to 32 hexadecimal digits, but can be summarized using a :: symbol. The ::1 is the IPv6 address for the localhost.

IPv4 Addresses consists of 32 bits. IPv4 addresses are written in dotted octet notation, such as 192.168.1.254.

MAC Addresses are written as a series of 12 hexadecimal digits, such as 00:AB:FA:B1:07:34. The other option, 192:168:1:55 is not a valid address since it uses : instead of a . in between the octets.

Ipv6 Stateless Address Autoconfiguration (SLAAC) is a mechanism that enables each host on the network to auto-configure a unique IPv6 address without any device keeping track of which address is assigned to which node. It's the preferred method of assigning IPv6 addresses, though DHCPv6 may be used.

Teredo is a transition technology that gives full IPv6 connectivity for IPv6-capable hosts that are on the IPv4 Internet but have no native connection to an IPv6 network.

DHCP & Default Gateway

Dynamic Host Configuration Protocol (DHCP) Server is a server configured with a range of addresses to lease. Hosts can be allocated an IP address dynamically or be assigned a reserved IP address based on their MAC address. The server can also provide other configuration information, such as the location of DNS servers.

DHCP IP Helper addresses enable a single DHCP server to provide DHCP IP addresses to every PC on the network, regardless of whether they are on the same broadcast domain as the DHCP server or not. DHCP IP Helper addresses are IP addresses configured on a routed interface such as a VLAN Interface or a routers Ethernet interface that allows that specific device to act as a "middleman" which forwards BOOTP (Broadcast) DHCP requests it receives on an interface to the DHCP server specified by the IP Helper address via unicast. Adding an IP Helper address to a new interface on a router will allow the DHCP broadcast requests to be forwarded to the workstations.

A Default Gateway is the node in an IP computer network that serves as the forwarding host (router) to other networks when no other route specification matches the destination IP address of a packet. It thus serves as an access point to another network, often involving not a change of addressing & networking technology. More narrowly defined, a router merely forwards packets between networks with different network prefixes. The networking software stack of each computer contains a routing table that specifies which interface is used for transmission and which router on the network is responsible for forwarding to a specific set of addresses. If none of these forwarding rules are appropriate for a given destination address, the default gateway is chosen as the router of last-resort. The default gateway can be specified by the route command, used to configure a node's routing table and default route.

Q: A network technician was tasked to install a network printer and share it with a group of five instructors at Dion Training. The technician plugged the device into a switch port and noticed the link light turned green. Unfortunately, the printer was unable to obtain an IP address automatically. Which of the following is a potential reason for this error?

A: DHCP scope is exhausted

Index

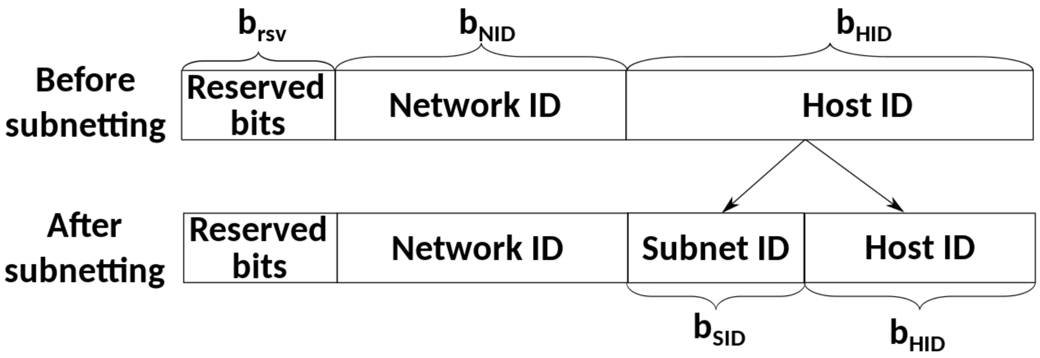
Subnetting

What is a subnet?

*A **subnetwork** or **subnet** is a logical subdivision of an IP network: The practice of dividing a network into two or more networks is called subnetting.*

Computers that belong to the same subnet are addressed with an identical Most-Significant Bit (MSB)-group in their IP addresses. This results in the logical division of an IP address into two fields: the network ID/number aka routing prefix and the host identifier / rest field, which identifies a specific host or network interface within the subnetwork.

Advantages of such splitting are primarily increased performance and improving security through isolation.

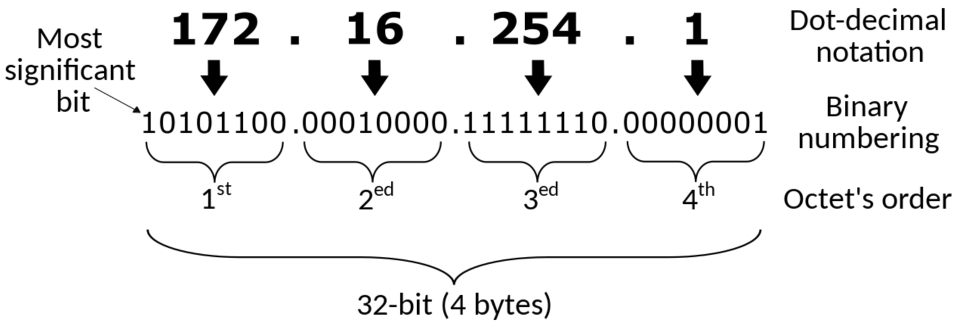


Quad-Dotted Decimal Notation

A notation used to represent unique IP addresses of computers on a TCP/IP network. It consists of **four integers separated by three dots**. Each integer is less than or equal to 255.

A dotted quad is thus a decimal representation of an IPv4 address that is human readable. It is represented in the form xxx.xxx.xxx.xxx. The number in each quad represents 1-byte / 8-bits in a 4-byte / 32-bit address.

For example, 192.168.0.1 would be an example of a dotted quad, also known as a dotted decimal or dot address.



Quad-Dotted: Basically 4 Octets separated by 3 dots

Index

Determining The Network Prefix and a Subnet's Network ID & Broadcast Address

The routing prefix may be specified in two ways:

1. Classless Inter-Domain Routing (CIDR) notation, written as the first address of a network, followed by a slash character (/) and ending with the bit length of the prefix. For example: 198.51.100.0/24 describes a network with the first 24 bits i.e. 3 octets reserved for the network prefix and the remaining 8 bits for host addressing. Addresses in the range of 198.51.100.0 to 198.51.100.255 belong to this network, with the first IPv4 address,198.51.100.0, in the network being the **network ID/address** and the last IPv4 address, 198.51.100.255, being the network's **broadcast address**.

2. Alternatively via a Subnet Mask / Netmask which when applied by a bitwise AND *(A ^ B: both A AND B must be True for a True result)* operation to any IP address in the network yields the routing prefix. For example for the IPv4 address above, 198.51.100.0/24, the subnet mask would be 255.255.255.0 (no subnet as no bits reserved for subnetting). Via the AND operation on this mask and any IP in the network, the network ID can be obtained:

Address	***Binary Representation***
198.51.100.23	*11000110.00110011.01100100.00010111*
255.255.255.0	*11111111.11111111.11111111.00000000*
Logical AND:	*11000110.00110011.01100100.00000000*
Network Address:	***198.51.100.0***

The host address can also be found like this: simply flip the bits of the subnet mask and perform the logical AND operation with the IP address!

Note:

- *A byte has 8 bits*
- *The max value for a byte is thus when all bits are set: 11111111*
- *Since we're referring to Binary notation, this is evaluated as powers of 2:*
  = 2^7 + 2^6 + 2^5 + 2^4 + 2^3 + 2^2 + 2^1 + 2^0
  = 128 + 64 + 32 + 16 + 8 + 4 + 2 + 1
  = 255
- *Remember, above we're converting from base-2 (binary) to base-10 (decimals), NOT figuring total number of combinations possible with 8-bits, though that too would be 2^8 = 256*

Index

Calculating the Network ID for a Given Address via the Subnet Mask or via Simple Division

Q: What is the network ID associated with the host located at 192.168.0.123/29?

- In this example, our CIDR IP address block is: 192.168.0.123/29
- An IPv4 address comprises 32-bits, represented as X.X.X.X, i.e. 4 octets of 8-bits each, where X can range from 0 to 255. Therefore, a single 8-bit octet can be any one of 256 numbers, ranging 0-255, as elaborated above.
- /29 means: 8 + 8 + 8 + 5
- In other words, 5-bits are used for subnetting, and 3-bits are left for the host within the subnets
- The subnet mask is therefore: 11111111.11111111.11111111.11111000
- Which computes as:
  - = 255.255.255. *(2^7 + 2^6 + 2^5 + 2^4 + 2^3 + 0 + 0 + 0)*
  - *= 255.255.255.(128 + 64 + 32 + 16 + 8 + 0 + 0 + 0)*
  - *= 255.255.255.248*
- Since 5-bits are used for subnetting, we can have a total of 2 ^ 5 = 32 subnets
- With 3-bits left over in the 8-bit octet, we can have 2 ^ 3 = 8 addresses per subnet
- Each subnet will have a network address and broadcast address: The first IP is the subnet's network address and the last IP it's broadcast address.
- Therefore, since we have 8 addresses per subnet, we can have 8 – 2 = 6 hosts per subnet
- This yields the following subnets:

192.168.0.0-192.168.0.7	192.168.0.8-192.168.0.15	192.168.0.16-192.168.0.23	192.168.0.24-192.168.0.31	192.168.0.32-192.168.0.39	192.168.0.40-192.168.0.47	192.168.0.48-192.168.0.55	192.168.0.56-192.168.0.63
192.168.0.64-192.168.0.71	192.168.0.72-192.168.0.79	192.168.0.80-192.168.0.87	192.168.0.88-192.168.0.95	192.168.0.96-192.168.0.103	192.168.0.104-192.168.0.111	192.168.0.112-192.168.0.119	**192.168.0.120-192.168.0.127**
192.168.0.128-192.168.0.135	192.168.0.136-192.168.0.143	192.168.0.144-192.168.0.151	192.168.0.152-192.168.0.159	192.168.0.160-192.168.0.167	192.168.0.168-192.168.0.175	192.168.0.176-192.168.0.183	192.168.0.184-192.168.0.191
192.168.0.192-192.168.0.199	192.168.0.200-192.168.0.207	192.168.0.208-192.168.0.215	192.168.0.216-192.168.0.223	192.168.0.224-192.168.0.231	192.168.0.232-192.168.0.239	192.168.0.240-192.168.0.247	192.168.0.248-192.168.0.255

Now, identify which subnet the given address, 192.168.0.123 falls into, and its lowest address is the network ID!

Index

Calculating the Network Address for ***192.168.0.123/29:***

Address	***Binary Representation***
192.168.0.123	*11000000.10101000.00000000.01111011*
255.255.255.248	*11111111.11111111.11111111.11111000*
Logical AND:	*11000000.10101000.00000000.01111000*
Network Address:	***192.168.0.120***

- RECAPPING!:
  - The given address is 192.168.0.123/29
  - /29 means: 8 + 8 + 8 + 5
  - 5-bits can therefore be used for subnetting, and 3-bits are left for the addresses within each subnet
  - Since 5-bits are used for subnetting, we can have 2 ^ 5 = 32 subnets
  - Since 3-bits are left for addresses within subnets, we can have 2 ^ 3 = 8 addresses per subnet
  - Since each subnet has a network address and a broadcast address, we can have 8 – 2 = 6 hosts per subnet
  - **With 8 addresses per subnet, and us requiring the network ID, i.e. the first address of the subnet the given IP falls into, we can simply divide 123 / 8 = 15.375, round down to the whole number 15 and multiply it by 8 to get 15 x 8 = 120, as explained below:**
  - The above works as we know the network is divided into 8-address subnets, so by dividing by 8, we get the approx. position of the address ending 123, which in this case happens to be somewhere in the 15th subnet (range 0-31). Now multiplying the number of addresses per subnet, 8, into the subnet number determined just now, 15, will yield the first address of the 15th subnet: 8x15=120!
  - Alternatively, we can calculate the network address by determining and using the subnet mask: with 5-bits for subnetting, we calculate our subnet mask as 255 . 255 . 255 . 11111000 = 255.255.255.248
  - With the subnet mask of 255.255.255.248 and the IP address of 192.168.0.123, we can calculate the Network ID via a simple Bitwise Logical AND operation to get 192.168.0.120

Index

Example 2: What is the network ID associated with 77.81.12.14/30?

- /30 translates to the following octets: 8 + 8 + 8 + 6
- 6-bits are used for subnetting
- 2 ^ 6 = 64 subnets!
- 2-bits reserved for addresses within subnets
- 2 ^ 2 = 4 addresses within each subnet
- 2 addresses reserved within each subnet for the Network ID and the broadcast address, therefore 4 – 2 = 2 hosts per subnet
- 4 addresses per subnet, so divide 14 / 4 = 3.xxx, and 4 x 3 = 12
- Therefore, the Network ID for the subnet associated with the IP address 77.81.12.14/30 = 77.81.12.12!
- Alternately, calculate the subnet mask. As 6-bits are reserved for subnetting, the mask may be calculated as: 255 . 255 . 255 . 11111100 = 255.255.255.252
- IP address: 77.81.12.14 and subnet mask: 255.255.255.252. Time for a Logical AND:

  If calculating in the exam, note down the reference bits:

  128 64 32 16 8 4 2 1

77.81.12.14 =	01001101.01010001.00001100.00001110
255.255.255.252 =	11111111.11111111.11111111.11111100
Logical AND =	01001101.01010001.00001100.00001100
Network ID =	77.81.12.12

Index

Q: You are configuring a point-to-point link and want to ensure it is configured for the most efficient use of your limited pool of available public IP addresses. Which of the following subnet masks would be BEST to use in this scenario?

A: /30

The most efficient subnet mask for a point-to-point link is actually a /31 subnet, which only provides 2 addresses. This will only work if both routers use a newer routing protocol like OSPF, IS-IS, EIGRP, or RIPv2 (or above). The most widely accepted and used method is to use a /30 subnet consisting of 4 IP addresses. The first is the network IP, the last is the broadcast, and the other 2 IPs can be assigned to the routers on either end of the point-to-point network. For the exam, if you see the option of /30 or /31, remember, they can be used for point-to-point networks.

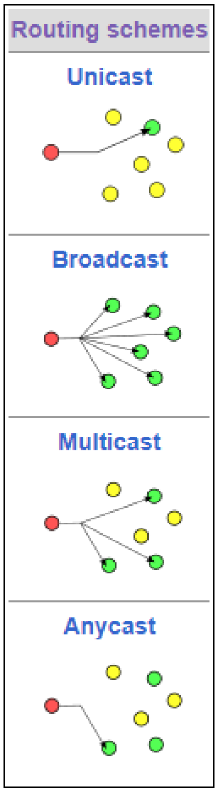
Q: Your company's corporate headquarters provided your branch office a portion of their Class C subnet to use at a new office location. You must allocate the minimum number of addresses using CIDR notation in order to accommodate each department's needs. What is the correct CIDR notation for the Human Resources (HR) department's subnet, which requires 25 devices?

A: /27

Since the Human Resources (HR) department needs 25 devices plus a network ID and broadcast IP, it will require 27 IP addresses. The smallest subnet that can fit 27 IPs is a /27 (32 IPs). A /27 will borrow 3 host bits and assign those to the network portion of the subnet mask. This would create a subnet with 2^5 available host IP addresses, or 32 total IP addresses. Of the 32 IP addresses, there are 30 available for clients to use, one for the network ID, and one for the broadcast address.

Index

IP Communication Types: Anycast, Unicast, Multicast and Broadcast



An IPv6 Anycast Address is an address that can be assigned to more than one interface (typically different devices). In other words, multiple devices can have the same anycast address**. A packet sent to an anycast address is routed to the “nearest” interface having that address**, according to the router’s routing table. Anycast communications are sent to the nearest receiver in a group of receivers with the same IP. **Anycast is not officially supported in IPv4 however, this can be worked around through using BGP.**

Multicasting is a technique used for **one-to-many communication** over an IP network. **Multicast can be used with both IPv4 and IPv6.**

Broadcast communication has one sender, but it sends the traffic to every device on the network. **Broadcast only works with IPv4.**

Unicast communication only has one sender and one receiver. **Works with IPv4 & IPv6.**

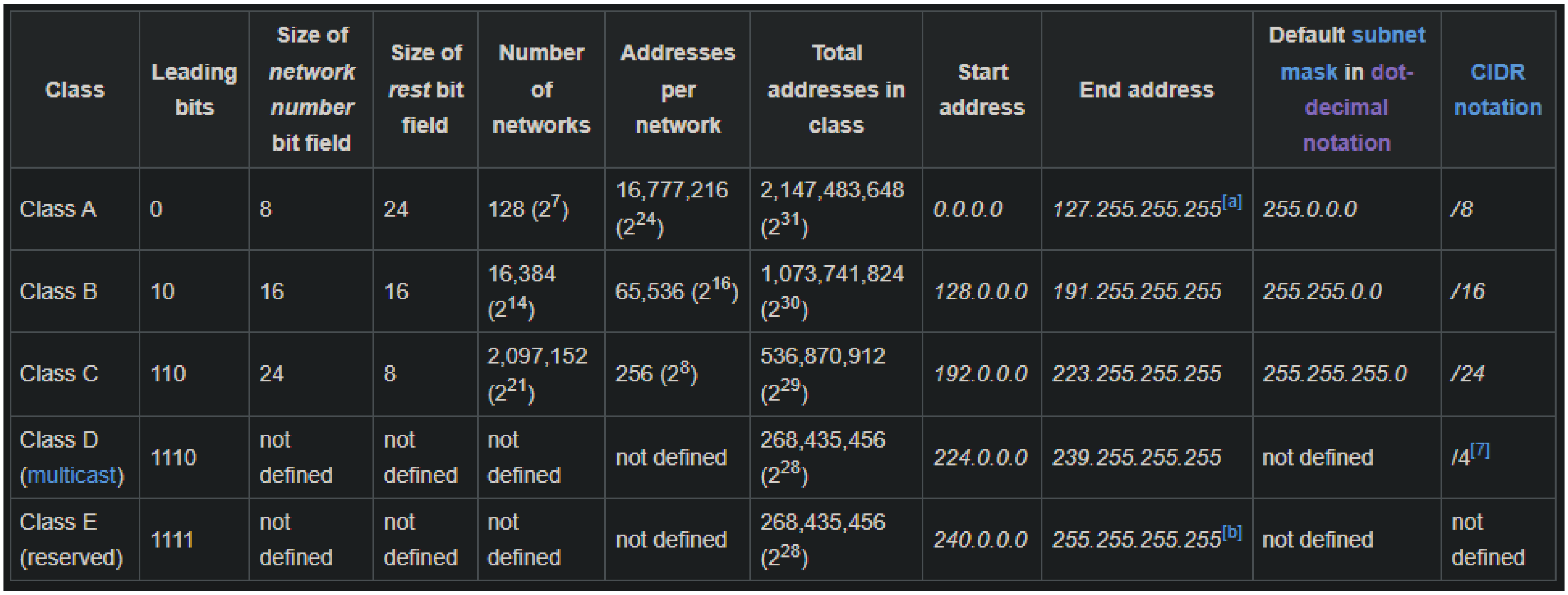
Q: Thomas has a server that streams media to the local network & the device is currently visible on the network. All of the workstations on the LAN can ping the device, and all the firewalls are currently turned off. The goal is for the streaming media server to allow different workstations to watch the stream if they choose to subscribe to it. The streaming device appears to be functioning properly, but the media won't stream when requested. Which of the following TCP/IP technologies is MOST likely not implemented properly?

A: Multicast

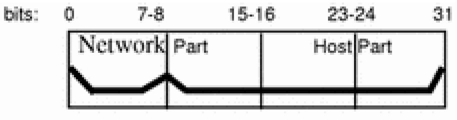
Multicast is a TCP/IP technology that sends out the packets to the requested devices when streaming to multiple workstations from a single streaming media server. As opposed to broadcast (one-to-all), which sends out packets to all devices, multicast (one-to-many-of-many/many-to-many-of-many) only sends packets to the clients that specifically requested to be a part of the distribution and not just every client on the network. Multicast requires the proper implementation and configuration to route the traffic to the right devices on the LAN so that streaming can properly function.

Index

Classful Addressing

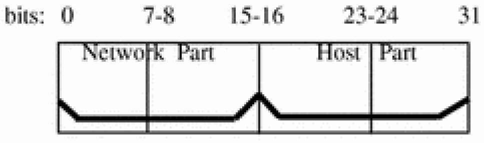


Class	Leading bits	Size of *network number* bit field	Size of *rest* bit field	Number of networks	Addresses per network	Total addresses in class	Start address	End address	Default subnet mask in dot-decimal notation	CIDR notation
Class A	0	8	24	128 (2^{7})	16,777,216 (2^{24})	2,147,483,648 (2^{31})	*0.0.0.0*	*127.255.255.255*[a]	*255.0.0.0*	*/8*
Class B	10	16	16	16,384 (2^{14})	65,536 (2^{16})	1,073,741,824 (2^{30})	*128.0.0.0*	*191.255.255.255*	*255.255.0.0*	*/16*
Class C	110	24	8	2,097,152 (2^{21})	256 (2^{8})	536,870,912 (2^{29})	*192.0.0.0*	*223.255.255.255*	*255.255.255.0*	*/24*
Class D (multicast)	1110	not defined	not defined	not defined	not defined	268,435,456 (2^{28})	*224.0.0.0*	*239.255.255.255*	not defined	*/4*[7]
Class E (reserved)	1111	not defined	not defined	not defined	not defined	268,435,456 (2^{28})	*240.0.0.0*	*255.255.255.255*[b]	not defined	not defined



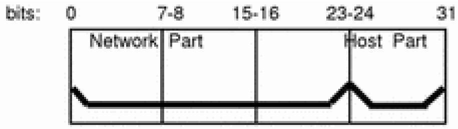
Class A Address

Class A Addresses are for networks with large number of total hosts: class A network number uses the first eight bits of the IP address as its "network part." The remaining 24 bits comprise the host part of the IP address



Class B Address

Class B Addresses are for medium to large sized networks: class B network number uses 16 bits for the network number and 16 bits for host numbers.



Class C Address

Class C Addresses are used in small local area networks (LA Ns) : Class C network numbers use 24 bits for the network number and 8 bits for host numbers. Class C network numbers are appropriate for networks with few hosts, the maximum being 254.

Q: A small real estate office has about 15 workstations and would like to use DHCP to assign classful IP addresses to each workstation. The subnet only has one octet for the host portion of each device. Which of the following IP addresses could be assigned as the default gateway?

A: 192.168.0.1

Since the question wants a classful IP addressing scheme to be assigned to devices, and only one octet being available for the host portion, it would need to be a Class C address. The only Class C address to choose from is 192.168.0.1 based on the options provided. The IP 10.0.0.1 is a Class A address. The IP 172.16.0.1 is a Class B address. The IP 169.254.0.01 is an APIPA (reserved) address. A non-routable IP address (in this case 192.168.0.1), also known as a private IP address, is not assigned to any organization and does not need to be assigned by an Internet Service Provider. Therefore, the 192.168.0.1 could be assigned to the outside local IP address of the router in a Network Address Translation based network.

Index

Legal Lemming

A legal hold is a process that an organization uses to preserve all forms of relevant information when litigation is reasonably anticipated. If a legal hold notice has been given to the backup service, **they will not destroy the old backup tapes until the hold is lifted.**

The process of discovery is the formal process of exchanging information between the parties about the witnesses and evidence they will present at trial.

The chain of custody is the chronological documentation or paper trail that records the sequence of custody, control, transfer, analysis, and disposition of materials, including physical or electronic evidence. It documents all changes in the control, handling, possession, ownership, or custody of a piece of evidence. The chain of custody is an important part of documenting the evidence collected during an incident response.

A data transport request is a formalized request to initiate a data transfer by establishing a circuit or connection between two networks.

eDiscovery is the term that refers to the process of evidence collection through digital forensics. eDiscovery is conducted during an incident response.

Q: When a criminal or government investigation is underway, what describes the identification, recovery, or exchange of electronic information relevant to that investigation?

A: eDiscovery

Separation of Duties is the concept of having more than one person required to complete a particular task to prevent fraud and error.

Dual Control, instead, requires both people to act together. For example, a nuclear missile system uses dual control & requires two people to each turn a different key simultaneously to launch a missile.

Mandatory Vacation Policies require employees to take time away from their job.

A Background Check is a process a person or company uses to verify that a person is who they claim to be and provides an opportunity to check a person's criminal record, education, employment history, and other past activities to confirm their validity.

Heavy Lifting

Lift with your legs, not your back and if it’s over 50 lbs., a coworker should be asked to assist with a team lift of the object!

Index

Forensic Investigation

As a forensic investigator, **you should always 'secure the area' before taking any other actions**. This includes ensuring that no other people are in the area to disrupt your forensic collection (such as the suspect or their accomplices), ensuring the workstation isn't unplugged from the network or the power, and other actions to prevent the evidence from being tampered with. **Once the area is secure, then you should document the scene, begin your evidence collection, and implement the chain of custody.**

Fire Suppression & Ventilation Systems

A fire Suppression System is an engineered set of components that are designed to extinguish an accidental fire in a workplace or datacenter.

A Wet Pipe System is the most basic type of fire suppression system, and it involved using a sprinkler system and pipes that always contain water in the pipes.

A Pre-Action System minimizes the risk of accidental release from a wet pipe system. With a pre-action system, both a detector actuation like a smoke detector and a sprinkler must be tripped prior to water being released.

Special suppression systems, like a Clean Agent System, use either a halocarbon agent or inert gas. When released, the agents will displace the oxygen in the room with the inert gas and suffocates the fire.

Heating Ventilation and Air Conditioning (HVAC) units are responsible for maintaining the proper temperature and humidity within a datacenter.

A Building Automation System (BAS) for offices and data centers ("smart buildings") can include physical access control systems, but also heating, ventilation, and air conditioning (HVAC), fire control, power and lighting, and elevators, and escalators.

Q: Which of the following types of fire suppression systems utilizes a sprinkler system with water to extinguish a fire but requires both an actuator and the sprinklers to be tripped prior to water being released?

A: Pre-Action Systems

Q: Which of the following types of facility controls is used to extinguish an accidental fire within a workplace or datacenter?

A: Suppression System

Q: Which of the following is used to remove heat from servers and networking gear within a datacenter?

A: HVAC

Index

Service-Level Agreement Guarantees

The Recovery Point Objective (RPO) is the interval of time that might pass during a disruption before the **quantity of data lost** during that period exceeds the Business Continuity Plan's maximum allowable threshold or tolerance.

The Recovery Time Objective (RTO) is the **duration of time** and a service level **within which a business process must be restored** after a disaster to avoid unacceptable consequences associated with a break in continuity.

The Mean Time To Repair (MTTR) measures the **average time it takes to repair** a network device when it breaks.

The Mean Time Between Failures (MTBF) measures the **average time between when failures** occur on a device.

Q: Which of the following terms represents the maximum amount of data, as measured in time, that an organization is willing to lose during an outage?

A: RPO. Do not confuse with RTO because it said time! RPO represents data loss, RTO refers to service recovery times.

Documents & Agreements

A Service Level Agreement (SLA) is a documented commitment between a service provider and a client, where the quality, availability, and responsibilities are agreed upon by both parties.

A Non-Disclosure Agreement (NDA) is a documented agreement between two parties that define what data is considered confidential and cannot be shared outside of that relationship. An NDA is used to protect an organization's intellectual property.

An Acceptable Use Policy (AUP) is a set of rules applied by the owner, creator, or administrator of a network, website, or service, that restrict how the network, website, or system may be used and sets guidelines as to how it should be used.

A Memorandum of Understanding (MOU) is a non-binding agreement between two or more organizations to detail what common actions they intend to take.

The Business Continuity Plan (BCP) focuses on the tasks carried out by an organization to ensure that critical business functions continue to operate during and after a disaster. It outlines how a business will continue operating during an unplanned service disruption. A business continuity plan is more comprehensive than a disaster recovery plan and contains contingencies for business processes, assets, human capital, and business partners, and essentially every other aspect of the business that might be affected.

EULA is an End-User License Agreement and is used during the installation of a piece of software.

Index

A Scope/Statement of Work (SOW) is a document that outlines all the work that is to be performed, as well as the agreed-upon deliverables and timelines.

Security Policy is a definition of what it means to be secure for a system, organization, or other entity.

A Disaster Recovery Plan is a documented, structured approach that documents how an organization can quickly resume work after an unplanned incident. These unplanned incidents include things like natural disasters, power outages, cyber-attacks, and other disruptive events.

An Incident Response Plan contains a set of instructions to help our network and system administrators detect, respond to, and recover from network **security** incidents. These types of plans address issues like cybercrime, data loss, and service outages that threaten daily work.

System Lifecycle Plans, also known as life cycle planning, describe the approach to maintaining an asset from creation to disposal. In the information technology world, we normally have a 5-phase lifecycle that is used for all of our systems and networks: Planning, Design, Transition, Operations, and Retirement.

Change Management Documentation authorizes changes and upgrades and should include the specific details of what was changed and what things may have been affected by the change. Change Management is a systematic approach to dealing with the transition or transformation of an organization's goals, processes, or technologies.

Q: You are assisting the company with developing a new business continuity plan. What would be the BEST recommendation to add to the BCP?

A: Build redundant links between core devices (NOT backups!)

By keeping redundant links between core devices, critical business services can be kept running if one link is unavailable during a disaster. Some of the other options are good ideas, too, but this is the BEST choice to maintain a high availability network that can continue to operate during periods of business disruption.

Q: Last night, your company's system administrators conducted a server upgrade. This morning, several users are having issues accessing the company's shared drive on the network. You have been asked to troubleshoot the problem. What document should you look at first to create a probable theory for the cause of the issue?

A: Change management documentation (NOT release notes for the server software, however more logical that sounds)

Q: Jason wants to use his personal cell phone for work-related purposes. Because of his position, Jason has access to sensitive company data, which might be stored on his cell phone during its usage. The company is concerned about this but believes that it might be acceptable with the proper security controls in place. Which of the following should be done to protect both the company and Jason if they allow him to use his personal cell phone for work-related purposes?

A: Conduct real-time monitoring of the phone’s activity and usage

Index

While all four are good options (NDA, AUP & occasional-monitoring), the BEST solution (though the question did not ask for it and instead stated “acceptable security measures”! WTF man?) is to conduct real-time monitoring of the phone's activity since it is a technical control that could quickly identify an issue. The other options are all administrative controls (policies), which are useful but would not actually identify if the sensitive data was leaked from Jason's phone.

Q: Which of the following policies or plans would dictate how an organization would respond to a fire that left their office building unusable for the next 3 months?

A: Disaster Recovery Plan

Easy to confuse for Business Continuity Plan (and I did in the mock test!), but the question asks about RESPONDING to a fire, NOT how operations will continue! A good note to end on then: READ THE QUESTIONS CAREFULLY!!!

Index