Networking

- Informational SOP Template - DO NOT USE
- SD-WAN - A Cloud-focused WAN routing technique
- How to factory reset a Cisco Meraki switch
- The OSI model and the basics of network troubleshooting
- How a network switch works
- How a router works
- How OSPF works
- How IS-IS works
- How BGP works
- MPLS - A WAN routing technique

Informational SOP Template - DO NOT USE

Author	Date	Revision
Author	04/18/2024	1.0

Related product (if any):	N/A
Description:	N/A
Notes:	N/A
Files Needed:	N/A
Information:	N/A

SD-WAN - A Cloud-focused WAN routing technique

Author	Date	Revision
Samuel Knoppe	04/23/2024	1.4

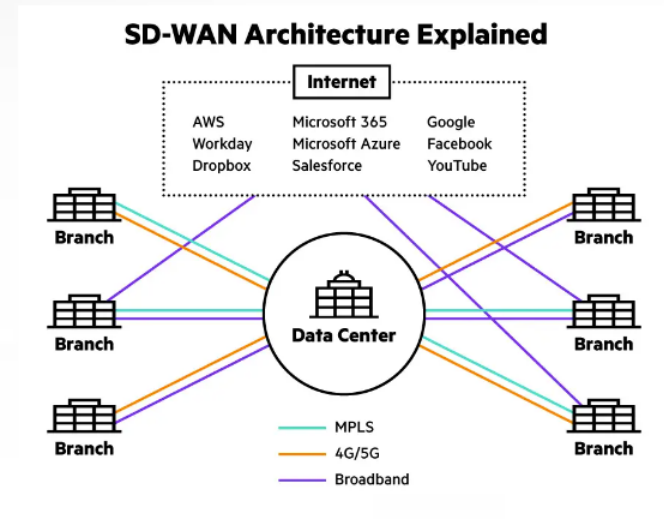
Related product (if any):	N/A
Description:	Describes SD-WAN and what it's used for.
Notes:	Knowledge of dynamic routing protocols, MPLS and WAN concepts, and the OSI Model will prove useful.
Files Needed:	N/A

Information:

What is SD-WAN?
Software-Defined Wide Area Networking (SD-WAN) architecture uses a centralized control function to steer traffic securely and intelligently across the WAN and directly to trusted SaaS and IaaS providers. This provides a more seamless experience and reduces costs for maintaining a more traditional WAN infrastructure, but the primary benefit is the enabled use of SaaS and IaaS services across the WAN. This is something like a traditional MPLS infrastructure cannot do natively with causing extra configuration and overhead.

Traditional WANs based on conventional routers weren't designed with the cloud in mind, and typically backhauled all traffic, including cloud-destined traffic, from branch offices to a hub or data center where advanced security inspection services can be applied. This delay caused by backhaul impairs application performance, resulting in poor user experience.

The SD-WAN model seeks to designed an architecture which fully supports applications hosted in on-premises data centers, public or private clouds, and SaaS services like Microsoft 365, Workday, Dropbox, and more. It supports these by providing the highest levels of performance.



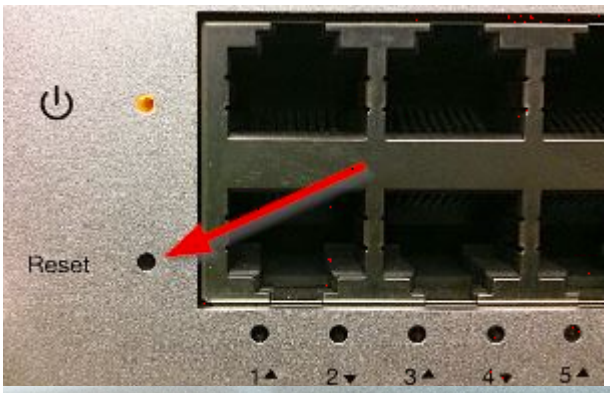
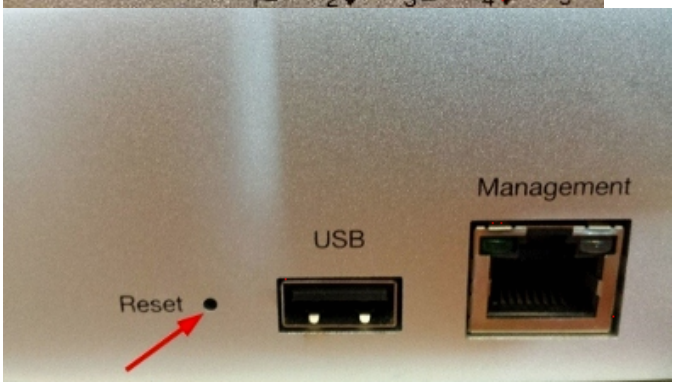
How does SD-WAN work?
Traditional conventional router-centric models for WAN distributes control functions across all devices in the network and simply routes traffic based on TCP/IP addresses and ACLs. This traditional model is rigid, complex, inefficient, and not cloud-friendly resulting in a suboptimal user experience.

SD-WAN is intended to deliver a superior application quality of experience (QoEx) for users. By identifying applications, an SD-WAN provides intelligent application-aware routing across the

How to factory reset a Cisco Meraki switch

Author	Date	Revision
Samuel Knoppe	4/9/2024	1.0

Related product (if any):	Cisco Meraki MS120, MS130, MS125, MS210, MS225, MS250, MS350, MS355, MS390, MS410, MS425, MS450
Description:	Shows the steps on how to factory reset a Cisco Meraki MS-series network switch.
Symptoms:	N/A
Cause:	N/A
Files Needed:	N/A

Steps to Correct:	1. Find a paper clip and locate the reset hole on the network switch. 2. Hold down the reset button for 10-15 seconds. The LED on the device will turn off. 3. The device will reboot and reset. It may take up to 5-10 minutes for the device to provision.  

The OSI model and the basics of network troubleshooting

Author	Date	Revision
Samuel Knoppe	4/10/2024	1.1

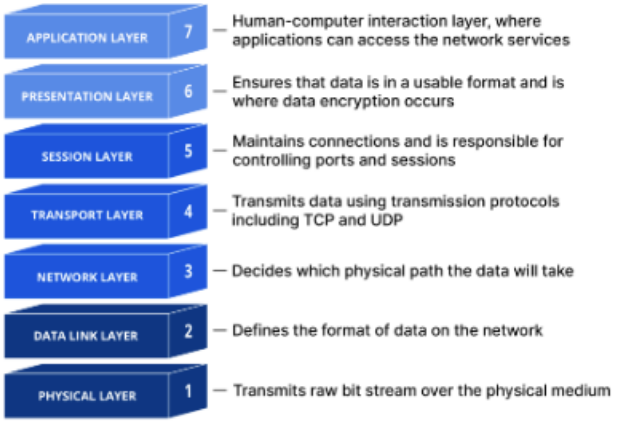
Related product (if any):	
Description:	Describes the open systems interconnection (OSI) model and how it is used for troubleshooting network-related issues in IT.
Symptoms:	
Cause:	
Files Needed:	

Steps to Correct:

The open systems interconnection (OSI) model is a conceptual model created by the International Organization for Standardization which provides a standard for different computer systems to be able to communicate with each other via standard protocols.

The OSI Model can be seen as a universal language for computer network. It is based on the concept of splitting up a communication system into seven abstract layers, each one stacked upon the last.

***The explanation of the layers and the OSI Model is copied from this CloudFlare article, or otherwise slightly abbreviated. This is not my work: https://www.cloudflare.com/learning/ddos/glossary/open-systems-interconnection-model-osi/**



Each layer of the OSI Model handles a specific job and communicates with the layers above and below itself. DDoS attacks target specific layers of a network communication; application layer attacks target layer 7 and protocol layer attacks target layers 3 and 4.

Understanding the OSI Model is vital for understanding how computer networking works, but it's also vital for troubleshooting networking-related issues. So let's start by breaking down what each layer does, starting from the top.

Layer 7: The application layer

This is the only layer that directly interacts with data from the user. Software applications like web browsers and email rely on the application layer to initiate communications. It's important to note that client software applications are not part of the application layer in their entirety; rather, the application layer is responsible for the protocols and data manipulation that the software relies on to present meaningful data to the user.

Some application layer protocols include HTTP/HTTPS and SMTP.

Layer 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

How a network switch works

Author	Date	Revision
Samuel Knoppe	4/11/2024	1.0

Related product (if any):	N/A
Description:	Explains the fundamentals of network switches, what they are used for, and how they work.
Symptoms:	N/A
Cause:	N/A
Files Needed:	N/A

Steps to Correct:

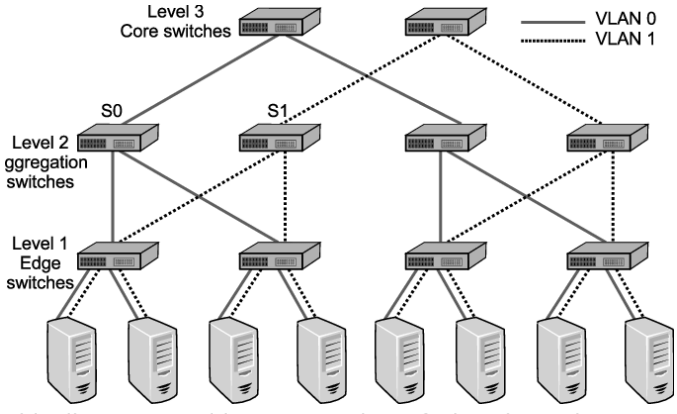
What is a network switch?
A network switch is a device which connects network devices and allows users to perform intra-network data exchange data packets via frames. Switches can be both hardware and software, and operate at Layer 2, the data link layer, in the OSI Model.

The way a switch operates is that it distributes information to the one device a frame is destined for, including some other switch, a router, or a user's computer, rather than several other devices in the network at once.

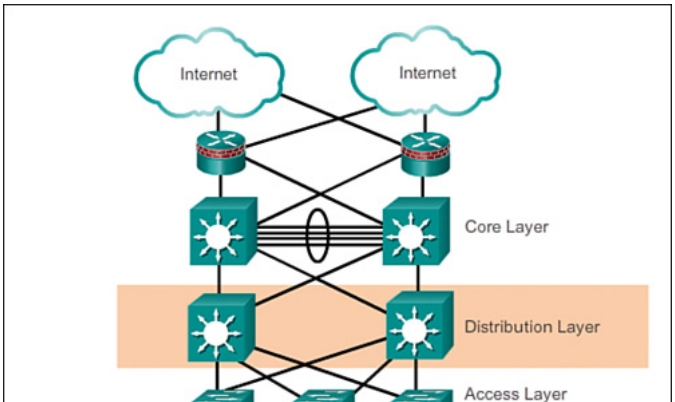
The majority of switches use Ethernet as its main Layer 1 medium of choice, but some also use fiber optics, InfiniBand, and more.

How does a network switch work?
Network switches can work in one of three ways in a network:

1. **Edge (or access) switches** handle traffic entering and departing the network. Edge switches link various devices like PCs and access points.
2. **Aggregation (or distribution) switches** are located within an optional intermediary layer in a network architecture. These connect to edge switches, which may transmit traffic from one switch to another or up to the core switches.
3. **Core switches** are the backbone of a network. Core switches link edge or aggregation switches, device or consumer edge networks to networks at data centers, and routers to organizational LANs.



This diagram provides an overview of what these three types of network switches will look like in a network architecture. This follows a design philosophy in network engineering calling the **3 Layer Hierarchical Network Model.**



How a router works

Author	Date	Revision
Samuel Knoppe	4/12/2024	1.0

Related product (if any):	N/A
Description:	Describes what a network router is, how it works, and some basic concepts relating to its functions.
Symptoms:	N/A
Cause:	N/A
Files Needed:	N/A

Steps to Correct:	**What is a router?** A router is a Layer 3 network device which routes IP packets. Without it, network devices will not be able to talk to each other. It facilitates communication by creating a local area network (LAN) which devices join, and it uses a **routing table** to route traffic to the Internet, and other remote networks. Routers differ from modems in that modems connect your home and business to Internet access via your ISP, whilst your router is the device which you actually connect to on your network--which your modem also connects to. **How does a router work?** A router figures out the fastest path between devices connected on a network, and sends data to those paths. To do this, routers use what's called a **metric value** or **preference number**. So if a router has to choose between two routes to the same location, it will choose the one with the lowest metric. Metrics are stored and shown in the routing table. P.S., there are different ways in which a router learns routes. Routes can be learned either **statically** or **dynamically** and generally speaking, static routes tend to have a higher preference when compared to a dynamic route. How a router chooses a route to a network via static route versus a route learned via a dynamic routing protocol, is via its **administrative distance (AD)**. So the flow is **Choose lowest AD route type/protocol > Choose route with lowest metric**. The **routing table** is a list of all possible paths in your network. When a router receives IP packets that need to be routed to another network, the router looks at the packet's IP address and then searches the routing table for routing information. Learning about routing tables is crucial for managing networks regardless of what protocols are being used. Managing routers involves making changes when necessary. This involves logging into your router via software, webpage, or through a terminal session. For example, you may need to change login passwords, encrypt the network, create port forwarding rules, or update the router's firmware. **NOTE: Traffic destined for another host on the same network will almost never go to the router. The network switch will used its forwarding information base (FIB) to send Layer 2 frames to the host instead.** **ARP and the routing table** Address Resolution Protocol (ARP) is a Layer 2 protocol that routers use to create a table that binds IP addresses to MAC addresses. Or in other words, it binds an IP address to the hardware device on the network. This is important since routers are normally Layer 3 devices on the OSI model. A router needs to know how an IP address relates to a Layer 2 MAC address, and ARP is how it figures this out. If a host wants to send a packet to another host via it's IP

How OSPF works

Author	Date	Revision
Samuel Knoppe	4/15/2024	1.1

Related product (if any):	Routers
Description:	Describes what OSPF is and how it works.
Symptoms:	N/A
Cause:	N/A
Files Needed:	N/A

Steps to Correct:	**What is OSPF?** Open Shortest Path First (OSPF) is an **Interior Gateway Protocol** used to distribute routing information within an **Autonomous System (AS)**. Or, in layman terms, it is a dynamic routing protocol used to distribute routes within internal networks. So... what the hell are those other things? Well, for starters, an **Autonomous System** refers to a collection of independent networks that are controlled by a single entity, such as an ISP. **Interior Gateway Protocols (IGPs)** are used to route traffic within each network of an AS, such as a company's LAN. There are three types of IGPs, including • Distance-vector routing protocols • Link-state routing protocols • Hybrid routing protocols A **distance-vector (DVR)** routing protocol calculates the best route based on distance. Distance is usually measured in hops, though the metric could be measured in delay, packets lost, or something similar. If the distance metric is a hop, then each time a packet passes through a router, a hop is considered to have traversed. The route with the least number of hops to a given network is concluded to be the best route to that network. Some examples of distance-vector routing protocols include: • Routing Information Protocol (RIP) • Interior Gateway Routing Protocol (IGRP) A **link-state routing protocol, also called shortest-path-first protocols,** have a complete picture of the network topology. Hence, they have a greater idea about the whole network than any distance vector protocol. Three separate tables are created on each link state routing enabled routing. One table is used to hold details about directly connected neighbors, another is used to hold the topology of the entire internetwork, and the last one is used to hold the actual routing table. Link state protocols send information about directly connected links to all the routers in the network. Some include: • OSPF • IS-IS (Intermediate System to Intermediate System) There also exists **hybrid** routing protocols in the sense that they used aspects of both distance vctor and link state protocols. • EIGRP (Enhanced Interior Gateway Routing Protocol) is one example of a hybrid routing protocol. So... what exactly *is* OSPF, then? And what's with all this preamble? Well, it's important to understand the distinction between IGPs and EGP (exterior gateway protocols--routes things over the Internet, basically), the concept of autonomous systems, and the difference between distance-vector and link-state protocols, because OSPF was made due to the need for a high functionality non-proprietary IGP for the TCP/IP protocol family. Now that you know these things, I can move forward.

How IS-IS works

Author	Date	Revision
Samuel Knoppe	4/18/2024	1.0

Related product (if any):	
Description:	Describes how the Intermediate-Systems to Intermediate-Systems (IS-IS) routing protocol works and what it is.
Symptoms:	N/A
Cause:	N/A
Files Needed:	N/A

Steps to Correct:	**What is IS-IS?** The IS-IS (Intermediate-Systems to Intermediate-Systems) protocol is an *interior gateway protocol (IGP)* that uses link-state information to make routing decisions. Just like OSPF, another IGP, it uses the shortest-path-first (SPF) algorithm to determine routes. IS-IS evaluates the topology changes and determines whether to perform full SPF recalculation or a partial route calculation (PRC). This protocol was orginally developed for routing **International Organization for Standardization (ISO) Connectionless Network Protocol (CLNP)** packets. Just like OSPF routing, IS-IS uses hello packets that allow network convergence to occur quickly when changes are detected. IS-IS uses SPF to determine routes. Using SPF, IS-IS evaluated network topology changes and determines if a full or partial route calculation is required. **The main difference between OSPF and IS-IS is that where OSPF requires IP configuration, IS-IS uses CLNP packets, which are connectionless, to send information.** **How does IS-IS work?** An IS-IS network is a single autonomous system (AS), also called a **routing domain**, that consists of *end systems* and *intermediate systems*. **End systems** are network entities that send and receive packets. **Intermediate systems** send and receive packets and relay (forward) packets. (Intermediate system is the Open System Interconnection [OSI] term for a router.) ISO packets are called network PDUs. Why are we discussing this terminology? Well, IS-IS doesn't use IP addresses like OSPF does, as mentioned above. The ISO developed CLNP packets and an entire suite of other functionality separate to that of IP to make a "connectionless" IGP. In IS-IS, a single AS can be divided into smaller groups called *areas*. Routing between areas is organized hierarchically, allowing a domain to be administratively divided into smaller areas. This organization is accomplished by configuring *Level 1* and *Level 2* intermediate systems. Level 1 systems route within an area; when the destination is outside an area, they route toward a Level 2 system. Level 2 intermediate systems route between areas and toward other ASs. No IS-IS area functions strictly as a backbone. Level 1 routers share intra-area routing information, and Level 2 routers share interarea information about IP addresses available within each area. Uniquely, IS-IS routers can act as both Level 1 and Level 2 routers, sharing intra-area routes with other Level 1 routers and interarea routes with other Level 2 routers. The propagation of link-state updates is determined by the level boundaries. All routers within a level maintain a complete link-state database of all other routers in the

How BGP works

Author	Date	Revision
Samuel Knoppe	04/19/2024	1.3

Related product (if any):	N/A
Description:	Describes what Border Gateway Protocol (BGP) is and what it does, and goes into detail about Exterior Gateway Protocols (EGPs) and how they relate to Interior Gateway Protocols (IGPs).
Notes:	95% copywrited from this CloudFlare article.
Files Needed:	N/A

Information:

What is BGP?

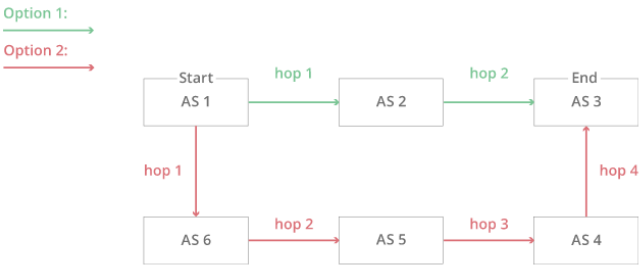
Border Gateway Protocol (BGP) is an Exterior Gateway Protocol (EGP) that makes the Internet work by enabling data routing between *autonomous systems (AS)*. BGP can be seen as the postal service for the Internet. When someone submits data via the Internet, BGP is responsible for looking at all of the available paths that data could travel and picking the best route.

BGP is generally considered a path-vector routing protocol, which sends peers information on which path traffic on a network will go. This includes which ASes that traffic will travel through. Distance-vector protocols like the IGP RIPv2 only counts hops, and is unable to know which exact path traffic will take.

BGP relies on path-vector route discovery due to the visibility it provides. This is also the reason why it's not a link-state routing protocol, since link-states do not have complete visibility and may introduce unwanted traffic via its LSU (link state update) packets, and so on. The IGP OSPF uses link-state routing.

Because BGP uses path-vector discovery, convergence times for BGP is the slowest among the routing protocols used today.

The Internet is a network of networks. It is broken up into hundreds of thousands of smaller networks known as **autonomous systems (AS)**. Each of these networks is essentially a large pool of routers run by a single organization. If we see BGP as the postal service of the Internet, ASes are like individual post office branches. A town may have hundreds of mailboxes. They forward outbound transmissions to the AS, which then uses BGP routing to get these transmissions to their destinations.



The above example illustrates a simplified version of BGP where there are only six ASes on the Internet. If AS1 needs to reach AS3, it has two different options:

1. Hopping from AS2 and then to AS3.
2. Or hopping to AS6, then to AS5, AS4, and finally to AS3.

This simplified version makes the decision seem straightforward. The first option has fewer hops

MPLS - A WAN routing technique

Author	Date	Revision
Samuel Knoppe	4/22/2024	1.0

Related product (if any):	N/A
Description:	Describes Multiprotocol Label Switching (MPLS) and how it works.
Notes:	Need perquisite knowledge of the OSI Model, network switching, network routing, EGPs and IGPs, OSPF, IS-IS, and BGP.
Files Needed:	N/A

Information:	**What is MPLS?** Multiprotocol label switching (MPLS) is a technique for speeding up network connections developed in the 1990s. Normally the public Internet forwards packets from one router to another, but MPLS sends packets along a predetermined network path. This ideally results in less time spend deciding where to forward each packet, since each packet takes the same path every time. Another way of looking at this is that MPLS defines different network paths instead of a series of intermediary destinations--routers. MPLS is considered to operate as OSI layer 2.5, so below the network layer (layer 3) and above the data link layer (layer 2). **How does MPLS work?** Normally anything sent from one network to another is divided up into smaller pieces called packets instead of getting sent all at once. For these packets to reach their intended destination each router hop must reference and maintain a routing table until the packet reaches the same network as its destination IP address. This approach works well in most cases, since most of the Internet runs using IP addresses and routing tables, but some organizations want their data to travel fast over paths they can directly control. The path a packet takes under the routing method can be different each time, but with MPLS packets take the same path each time. The way this is done in a network that uses MPLS is that each packet is assigned a **forwarding equivalence class (FEC)**. The network paths that packets can take are called **label-switched paths (LSP)**. A packet's class (FEC) determines which path (LSP) the packet will be assigned to. Packets with the same FEC will follow the same LSP. Each packet can contain one or more labels, and all labels are contained in an MPLS header, which is added on top of all of the other headers attached to a packet. FECs are labeled within each packet's labels. Routers do not examine the other headers; meaning, they can essentially ignore the IP header entirely. Instead, they examine the packet's label and direct the right packet to the right LSP. Because MPLS-supporting routers only need to see the MPLS labels attached to a packet, MPLS can work with any protocol, hence the name. It doesn't matter how the rest of the packet is formatted as long as the router can read the MPLS labels at the front of the packet. So for instance, you can have traffic routed via BGP be encapsulated within an MPLS header.