Official Cert Guide

Study Planner

CCNP and CCIE Collaboration Core

CLCOR 350-801

2nd Edition

ciscopress.com

Jason Ball, CCSI® No. 33717

Companion Website and Pearson Test Prep Access Code

Access interactive study tools on this book's companion website, including practice test software, review exercises, a Key Term flash card application, a study planner, and more!

To access the companion website, simply follow these steps:

1. Go to **www.ciscopress.com/register**.
2. Enter the **print book ISBN:** 9780138200947.
3. Answer the security question to validate your purchase.
4. Go to your account page.
5. Click on the **Registered Products** tab.
6. Under the book listing, click on the **Access Bonus Content** link.

When you register your book, your Pearson Test Prep practice test access code will automatically be populated in your account under the Registered Products tab. You will need this code to access the practice test that comes with this book. You can redeem the code at **PearsonTestPrep.com**. Simply choose Pearson IT Certification as your product group and log in to the site with the same credentials you used to register your book. Click the **Activate New Product** button and enter the access code. More detailed instructions on how to redeem your access code for both the online and desktop versions can be found on the companion website.

If you have any issues accessing the companion website or obtaining your Pearson Test Prep practice test access code, you can contact our support team by going to **pearsonitp.echelp.org**.

Foundation Topics

LAN, WAN, and Wireless LAN

The most foundational components of any corporate communication solution are the network infrastructure components. One of the reasons Cisco is the leader in the collaboration market is that only Cisco can offer an end-to-end solution to its customers. Of course, providing superior collaboration products with extensive capabilities and beautiful designs helps contribute to the company's ability to hold that leading position. The purpose of this chapter is not to provide an extensive education on these network components and how to configure them. However, there is such a close dependency on Cisco collaboration products and the network that it is essential to have an understanding of the network to a certain level. To provide a deeper understanding of basic networking components, Cisco offers the CCNP Enterprise certification courses, which can also be studied using the Cisco Press material. These courses and the material will provide a more thorough understanding of what each network component is and how to configure it. For the purposes of this book, we will examine the foundational network infrastructure components because they relate directly to the Cisco preferred architecture for enterprise collaboration.

A network can be defined as a group or system of interconnected things. A local-area network (LAN) is a network of devices within a limited area. This could be a business office, school, or campus. A home network is a LAN that might interconnect computers, smartphones, tablets, smart TVs, printers, and other media devices. A wide-area network (WAN) is a network of devices within a wider area than the LAN. Imagine two LAN offices, one located in New York City and the other in Washington DC, but devices within each of these locations can communicate with one another as if they were within the same LAN. This is a WAN. Then there is the wireless local-area network (WLAN) or wireless LAN. Because different technologies exist within wireless technology as compared to a physical LAN, this type of network must be categorized independently. Most home networks use some sort of consumer wireless router, but the technology behind a commercial wireless LAN goes far beyond what is available to the everyday consumer.

Now that we've defined the different types of networks, let's examine some of the physical network components and how they might be used. The only network component needed to set up a LAN is a switch. A basic switch is a device with multiple physical ports to which multiple devices can be connected using an Ethernet cable so that communication between these devices can be established. Switches operate on Layer 2 of the OSI model. Cisco switches have a higher level of intelligence than a basic switch, so a network administrator can configure parameters that control how traffic flows through these switches. In fact, some of the switch models that Cisco offers can be configured with Layer 2 and Layer 3 capabilities. As switches pertain to collaboration, several configuration elements can be configured, including virtual LANs (VLANs), Cisco Discovery Protocol (CDP), Link Layer Discovery Protocol-Media Endpoint Discovery (LLDP-MED), and quality of service (QoS), to name a few. As essential as a switch is within a network, you cannot access the public Internet or establish a WAN without the next network component—the router.

Routers are Layer 3 components of the OSI model and provide communication into and out of the LAN. Many services can be provided through a router. Routers are often configured

to offer Dynamic Host Configuration Protocol (DHCP) services to devices on the network. DHCP provides devices with an IP address, subnet mask, and default gateway (also known as the default router) address at a minimum. It can also provide Domain Name System (DNS) address(es) and Trivial File Transfer Protocol (TFTP) server address(es). Devices connected to a switch know how to route traffic to a router using the Default Gateway Address, which is the internal IP address of the router. TFTP addresses can be provided using Option 66 or the Cisco proprietary Option 150.

Because a LAN operates using private IP addresses, which are not publicly routable, the router can masquerade these private IP addresses with a public IP address so that traffic can be routed out to the public Internet. The service used to masquerade these addresses is known as Network Address Translation (NAT) or Port Address Translation (PAT). Many devices on the network require the timing to be synchronized for services to operate properly, such as endpoints joining a scheduled meeting. Therefore, these networked devices rely on Network Time Protocol (NTP) to provide timestamp information. When the edge router is configured as the NTP authority, it can provide a Stratum 2+ NTP reference to these devices.

Firewall software is typically also available on routers. Some companies opt for a firewall server in lieu of, or in addition to, the firewall software available on the router. Firewalls protect nodes within your network from malicious attacks coming from outside your network. Think of firewalls as a first line of defense. Other defensive control mechanisms available on the router are access control lists (ACLs). ACLs are lists of protocols and port numbers that are allowed or not allowed to flow through a router. ACLs can be applied on an inbound or outbound (physical) port on the router. For example, an ACL could be configured on a router that allows TLS traffic on port 5061 but rejects TCP traffic on port 5060. The idea here is to allow encrypted SIP signaling and reject nonencrypted SIP signaling. ACLs can also be used as a stateless inspection of the traffic, which differentiates ACLs from firewalls.

Routers offer many more features, but one last feature worth mentioning is QoS. As mentioned previously with Layer 2 switches, QoS can be applied at Layer 3 on the router. In fact, Layer 3 QoS is even more critical than Layer 2 QoS because this is typically where you will find congestion in a network. Ideally, you want to mark packets as close to the source as possible; therefore, Layer 2 QoS is designed to mark packets early in the routing process. Layer 3 QoS prioritizes how traffic will flow during these high-congestion times. On the router, you need to convert Layer 2 QoS marking to Layer 3 QoS marking. Other Layer 3 tools for QoS include shaping, policing, queuing, and QoS type. Cisco has a lot of information available on QoS, and it is essential to research and understand QoS to work effectively in collaboration as a technician or engineer. QoS will be covered in a little more depth in the next chapter, although QoS is a very deep topic that could fill volumes of books all on its own.

Among Cisco routers, one stands out above the rest: the Cisco Integrated Services Router (ISR). The ISR has all the same services that other routers have, as mentioned previously. However, additional services and modules can be added to the ISR. Some of the collaboration services available on an ISR include Cisco Unified Communications Manager Express (CUCME), Survivability Remote Site Telephony (SRST), Cisco Unified Border Element

(CUBE), and Cisco Unity Express (CUE). Modules that are supported in select models of ISRs include PRI cards (E1 and T1), FXS and FXO cards, and PVDM cards.

Key Topic

Collectively, Cisco is known as "The Network People" for a reason. It offers the best proven network products available on the market. Over 80 percent of the public Internet space consists of Cisco networking products. And the company is continually releasing software advancements on its network products that push the edge of what is possible. One such software advancement that provides added intelligence to your network is known as Medianet. Cisco Medianet can be defined as an end-to-end architecture for a network comprising advanced, intelligent technologies and devices in a platform optimized for the delivery of rich-media experiences. Medianet allows network devices to be media-aware so that they can detect and optimize different media and application types to deliver the best experience to the user, such as Telepresence, video surveillance, desktop collaboration, and streaming media, to name a few. Medianet also makes networking devices endpoint-aware to automatically detect and configure media endpoints. Finally, Medianet makes networking equipment network-aware so that it can detect and respond to changes in device, connection, and service availability. With the increasing adoption of new video and rich-media applications, Medianet technologies become critically important to address challenges associated with the transmission of video, voice, and data over the network, including ensuring predictability, performance, quality, and security. By accelerating deployment of applications, minimizing complexity and ongoing operational costs, increasing visibility into the network, and helping to scale the infrastructure for the best quality of experience, Medianet technologies help address these challenges. Check out the Cisco Medianet Data Sheet at Cisco.com for more information on Medianet.

Depending on the environment being configured, there might be a need for Layer 2 switches, Layer 3 switches, and Layer 3 routers. A large enterprise network can be divided into four layers at the central office and two layers at a branch office. The central office can be divided into the Access layer, Distribution layer, Core layer, and the WAN Aggregation layer. The Access layer is typically made up of Layer 2 switches. The Distribution layer is typically made up of Layer 3 switches. The Core layer can be made up of Layer 3 switches or Layer 3 routers. The WAN Aggregation layer is always a Layer 3 router. The branch office typically utilizes a branch router and a branch switch to form the two layers needed for communication. Figure 12-1 illustrates how a typical enterprise network infrastructure is designed.

LAN

A properly designed LAN will take into consideration the needs for high availability and quality of service. This will account for the Access layer, Distribution layer, and Core layer of the typical enterprise network infrastructure. The Access layer offers in-line power to the phones, multiple queue support, 802.1p and 802.1q, and fast link convergence. The Distribution and Core switches offer multiple queue support as well as 802.1p and 802.1q, the same as the Access layer, along with traffic classification and reclassification. An IEEE protocol, 802.1p refers to the support of QoS on Layer 2 switches. Also an IEEE protocol, 802.1Q refers to the support of virtual LANs on Layer 2 switches.

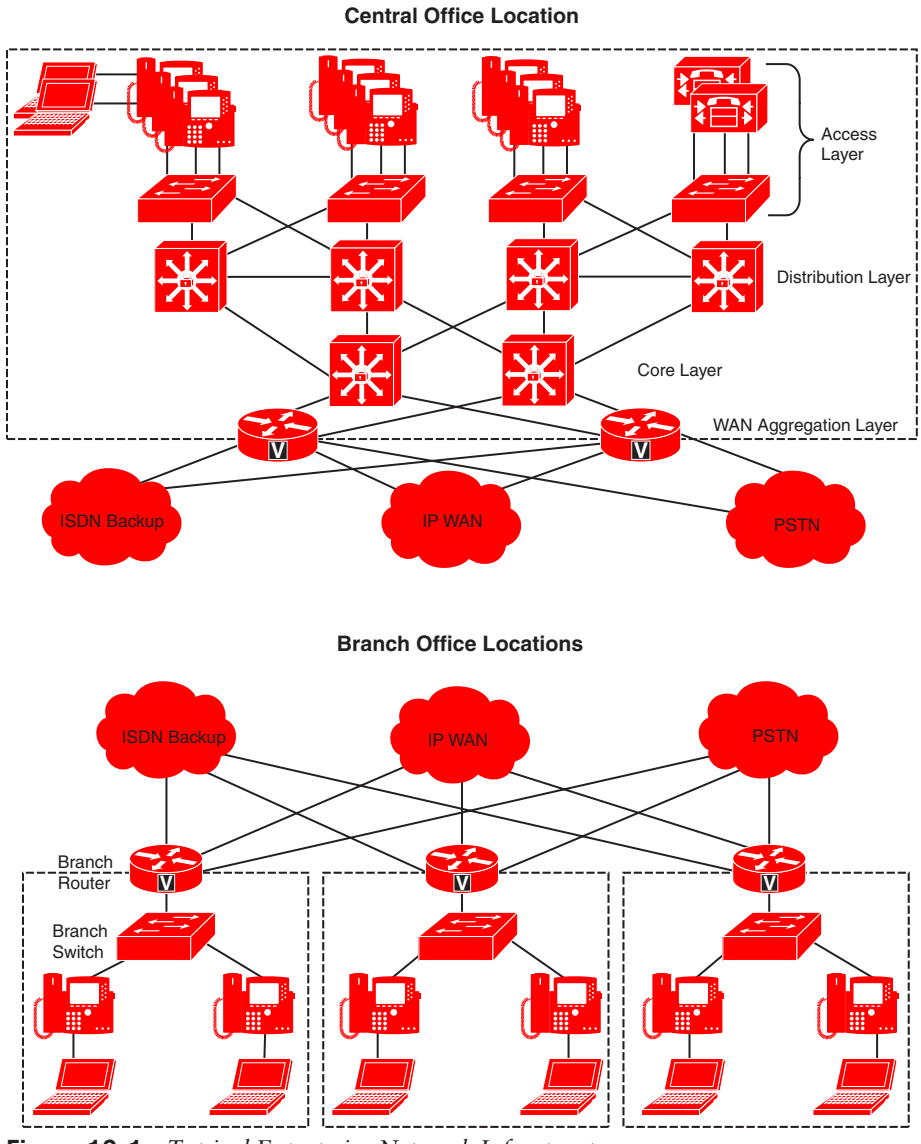

Figure 12-1 *Typical Enterprise Network Infrastructure*

Access Layer

Key Topic

High availability can be configured on the Access layer by using the Spanning Tree Protocol (STP). STP is a Layer 2 protocol that runs on switches and is specified by the IEEE standard 802.1d. The purpose of STP is to prevent loops when configuring redundant paths within the network. In Figure 12-1, observe that each switch is connected to two or more other switches, so that if one path fails, there is a redundant path to the destination. On the switch ports, STP can be configured to block traffic on one port and forward traffic on the other port. In the event that the forwarding port can no longer send and receive communications, the state of the blocking port will change to allow the data to flow along the alternate path.

This ensures that there is an alternate path for routing traffic but eliminates the chance of a loop occurring with two open ports. Different flavors of STP can be used, and each one requires different timing for convergence. Therefore, it is recommended that the same version of STP be used within a single environment. Some of the other Spanning Tree Protocols that exist include IEEE 802.1w Rapid Spanning Tree Protocol (RSTP) and IEEE 802.1s Multiple Instance Spanning Tree Protocol (MISTP). These two can converge at much higher rates than the traditional STP.

Key Topic

A virtual local-area network, or VLAN, is another essential part of the Access layer switch, and it should be configured prior to setting up STP. A VLAN is a logical grouping of devices connected to the switch that allows data traffic in the network to be decoupled for access control and prioritization. VLANs can be used to group devices in several ways, such as device type or department. For example, there may be a server where accounting software resides. The accounting team needs access to this software, but the sales team does not need access. The accounting team also needs to be able to communicate with the sales team for handling expense reports. In this scenario, three VLANs can be used to control who can access the accounting software. The server where the software resides can be placed in VLAN110, the accounting team computers can be placed in VLAN120, and the sales team computers can be placed in VLAN130. Then the network administrator can create connections from VLAN120 to VLAN110, and from VLAN120 to VLAN130. This will allow the accounting team to access the accounting software and communicate with the sales team. However, the sales team will be restricted from accessing the accounting software.

In a Cisco collaboration environment, VLANs are essential to implementing proper QoS. At least two VLANs should be created in this environment: a data VLAN and a voice and video VLAN, which is typically signified as VVID (Voice VLAN ID). Voice and video data can traverse the same VLAN, even though they typically experience different QoS markings. The reason these two VLANs need to be created is that Cisco phones have a NIC connecting the phone to a switch and a computer NIC connecting a computer to the phone. The phone and the computer require different QoS treatment and therefore should belong in different VLANs. This is where the configuration gets really interesting. If the phone is connected to the switch and the computer is connected to the phone, how can they possibly be decoupled into different VLANs? On the port at the switch where the phone is connected, both the Data VLAN and the VVID can be assigned. When the phone boots up, CDP or LLDP-MED can be used to discover both of these VLANs. There is a third virtual NIC in the phone that exists to monitor egress traffic and determine which VLAN should be used. Data traffic sourced from the computer will use the Data VLAN. Voice and video data from the phone will use the VVID. If content is being shared from the computer during a video call, then the VVID will be used for that particular data sourced from the computer.

One final offering that can be utilized at the Access layer needs to be mentioned here: inline power. Inline power, or Power over Ethernet (PoE), has already been discussed at great length. For a review of the information coving PoE, refer to Chapter 9, “Endpoint Registration.” Table 12-2 outlines the different types of PoE and the maximum power available. Some examples of Cisco switches that support the different types of PoE can also be found in Table 12-2.

Key Topic

Table 12-2 PoE Types and Supported Power

PoE Type	PoE Power Capabilities	Example Switches
Pre-Standard Inline Power	6.3 Watts power	3550-24 or 48 ports
802.3af PoE	15.4 Watts power (Type 1)	3560-24 ports or 3670-48 ports
802.3at PoE	30 Watts power (Type 2)	2960-24 is Type 1 or Type 2
	60 Watts power (Type 3)	4500 supports all types of PoE
	100 Watts power (Type 4)	9000 supports all types of PoE

Distribution Layer

The Distribution layer switches can offer the same multiple queue support, 802.1p, 802.1q, and fast link convergence as the Access layer. However, the focus of the Distribution layer should be to offer Layer 3 routing, load balancing, and fault tolerance. These Distribution layer switches are the bridge between Layer 2 and Layer 3 of the enterprise network.

Key Topic

The Distribution layer switch can often serve as the Layer 3 default gateway for the Layer 2 devices. Should the Distribution layer switch fail, then many devices could lose communication across the network. Cisco initially released the Hot Standby Router Protocol (HSRP) to provide a fault-tolerant default gateway. The IETF developed a similar protocol called the Virtual Router Redundancy Protocol (VRRP) with RFC 5798. Although these two protocols are similar in nature and resolve the gateway redundancy issue, they are not compatible protocols and they each have some limitations. Cisco overcame these limitations when it released another protocol called the Gateway Load Balancing Protocol (GLBP). This protocol protects data traffic from a failed router or circuit, while also allowing packet load sharing between a group of redundant routers.

Endpoints use the Address Resolution Protocol (ARP) to learn the physical MAC address of their default gateway. With HSRP, a single virtual MAC address is provided to these endpoints. With GLBP, two virtual MAC addresses can be provided to the endpoints—one from the primary gateway and one from a peer gateway—which are distributed using round-robin technique.

Another way to ensure fast convergence, load balancing, and fault tolerance on the Distribution layer is to use Layer 3 routing protocols such as OSPF or EIGRP. You can use parameters such as routing protocol timers, path or link costs, and address summaries to optimize and control convergence times as well as to distribute traffic across multiple paths and devices. Cisco also recommends using the **passive-interface** command to prevent routing neighbor adjacencies via the access layer. These adjacencies are typically unnecessary, and they create extra CPU overhead and increased memory utilization because the routing protocol keeps track of them. By using the **passive-interface** command on all interfaces facing the access layer, you prevent routing updates from being sent out on these interfaces, and therefore, neighbor adjacencies are not formed.

Core Layer

The Core layer operates entirely in Layer 3 of the enterprise network. This layer can consist of Layer 3 switches or routers. The purpose of the Core layer is to provide redundancy between different Distribution switches. In the event of network outages, the Core layer can redirect traffic along a more stable path. The types of redundancy that need to be provided at the Core layer include Layer 1 link paths, redundant devices, and redundant device subsystems, such as power supplies and module cards. The Cisco Catalyst switches with