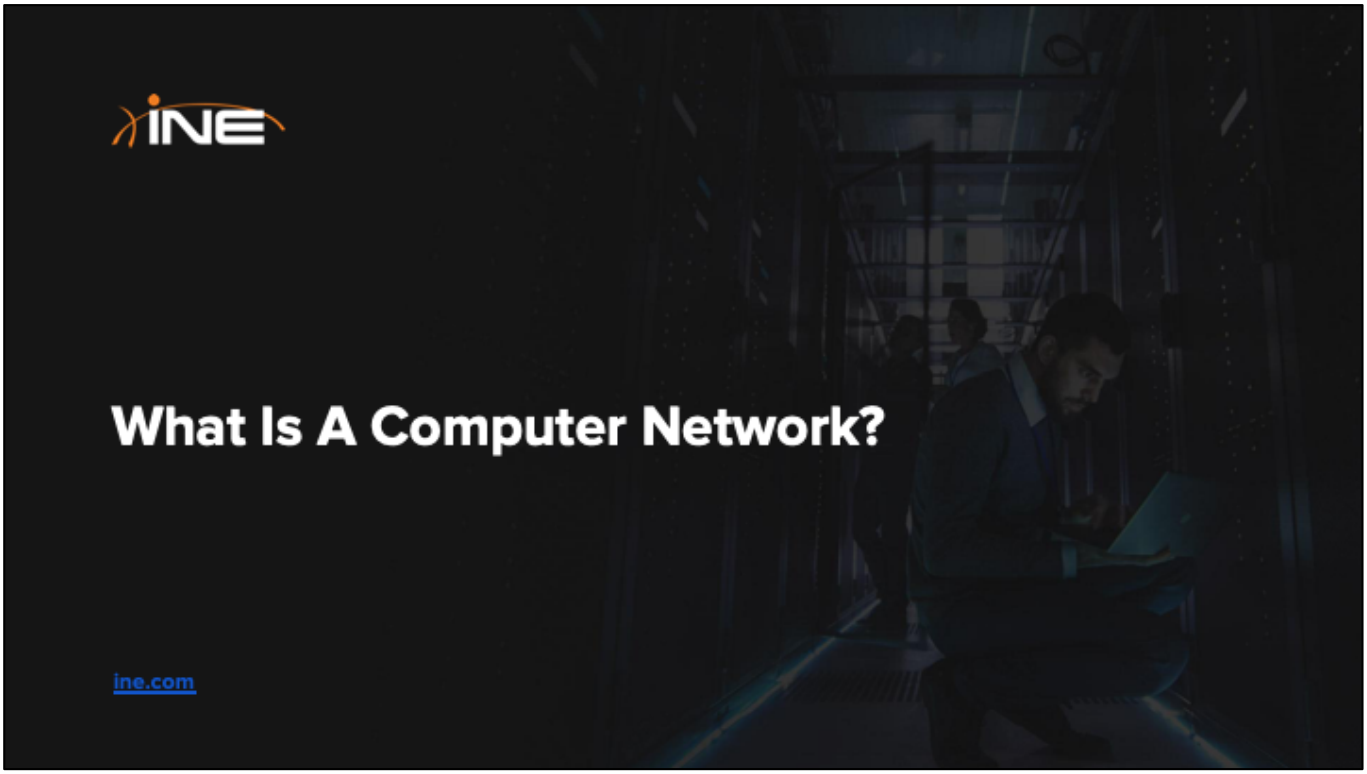
Who This Course Is For

+ Those thinking of pursuing a career in computer networking, but are still investigating, this course will identify what a computer network is, and common components of a computer network

What is a Computer Network?
Components of a Computer Network
Technologies That Comprise a Network.
Computer Networking Job Roles
Computer Networking Job Specialties
Where Do I Go From Here?

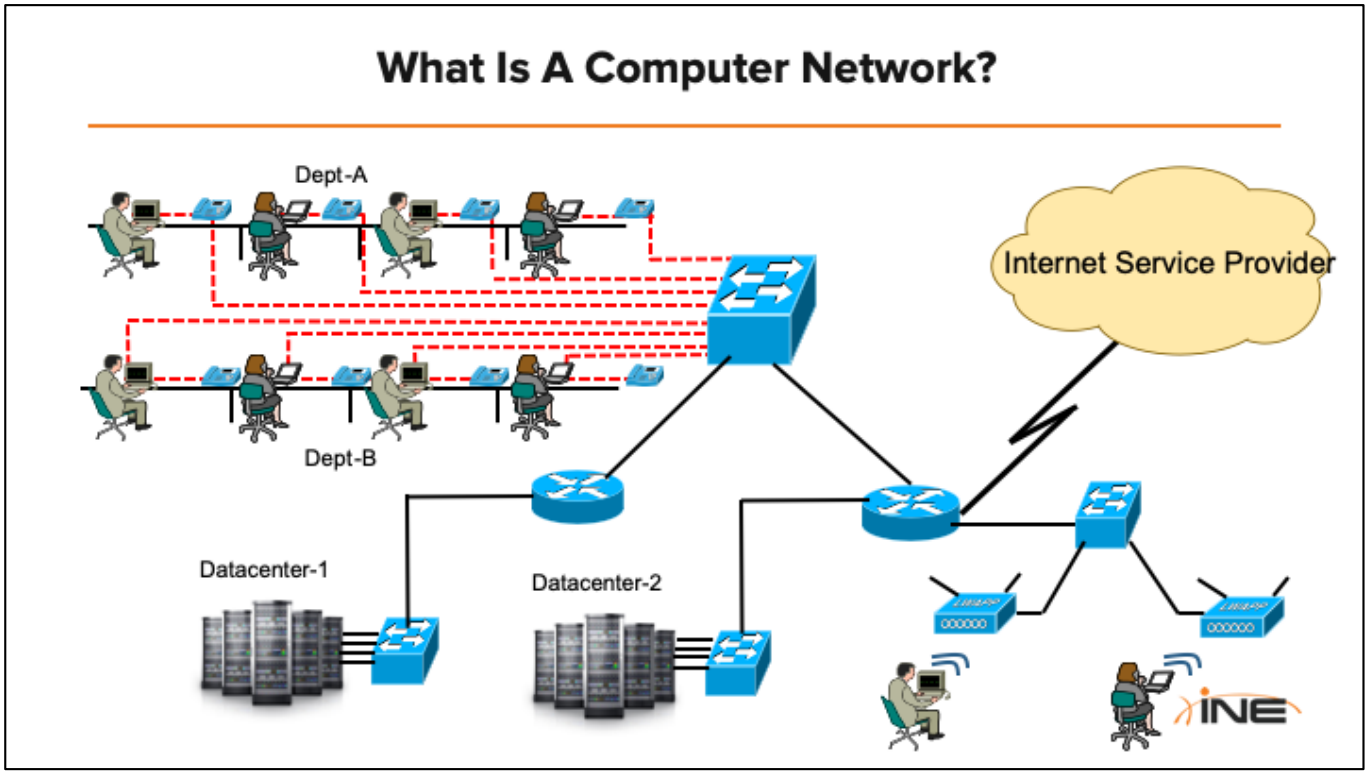
+ A Desire To Learn
+ Basic Familiarity With A Computer

Course Prerequisites



Topic Overview

- The Parts Of A Common Computer Network
- Common Vocabulary You Need To Know
- Why Do We Need Computer Networks?



A network is nothing more than two or more computing devices connected by a cable or by a wireless radio connection so that they can exchange information

1. Prior to networking, individual users…SNEAKERNET!

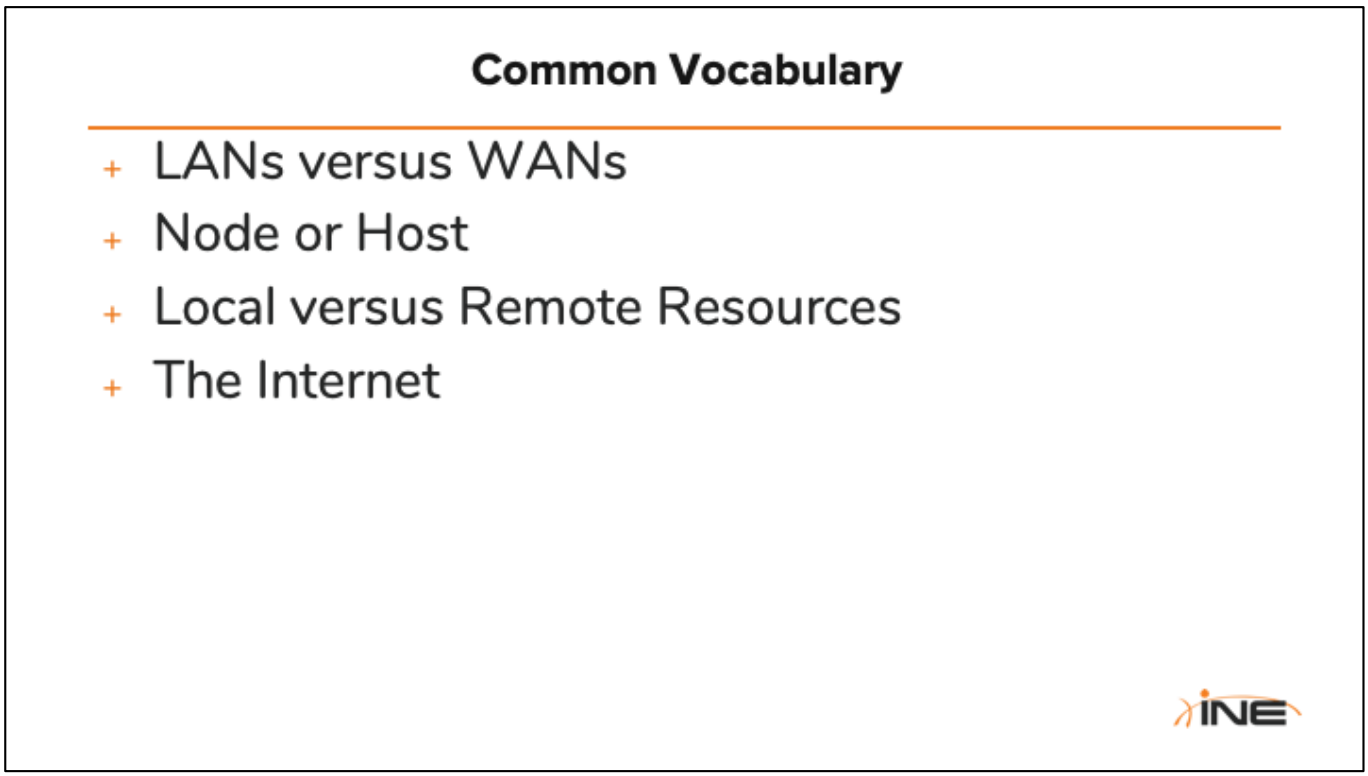
2. Phones had their own network, now we have IP phones.

3. All of those host devices are cabled into what we call the network infrastructure

4. You'll probably also have users and devices that utilize WiFi to connect to infrastructure

5. Your company may also have a datacenter (explain the term)

6. Lastly, don't forget the internet connection.



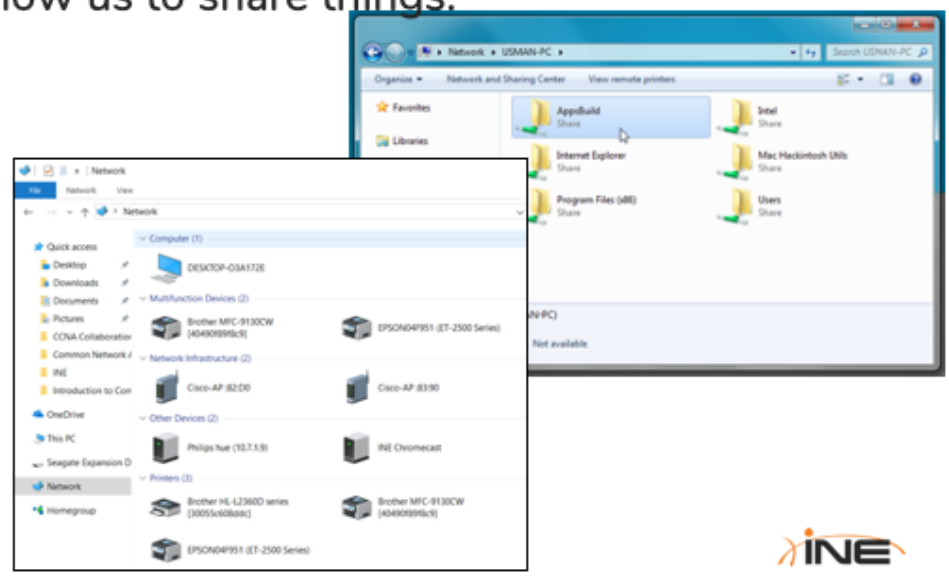
Common Terms/Vocabulary

-

Any device that is connected to the network is called a node

Why Do We Need Computer Networks?

- Networks allow us to share things:
- Files
- Programs
- Resources



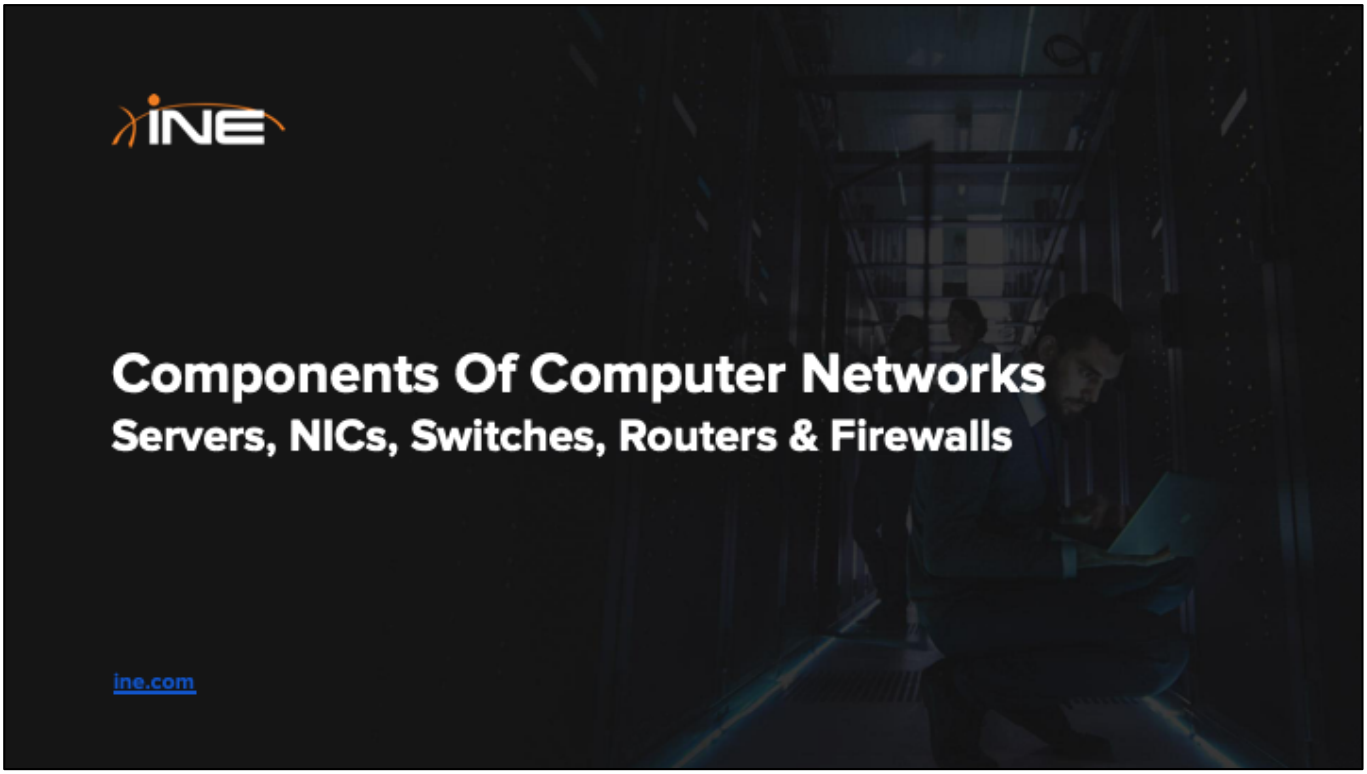
When you download a new app for your phone or tablet, it's the network that makes that possible.

-

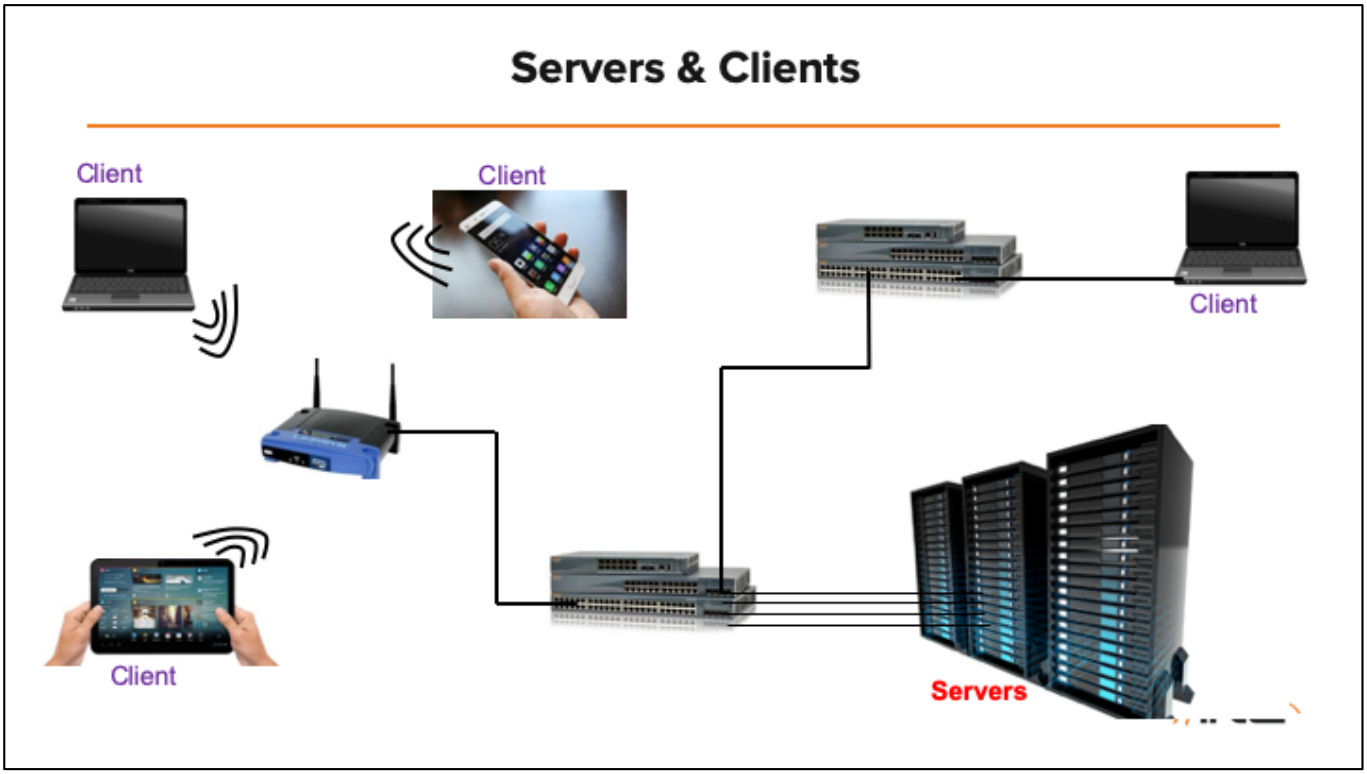
Resources:

----Printers

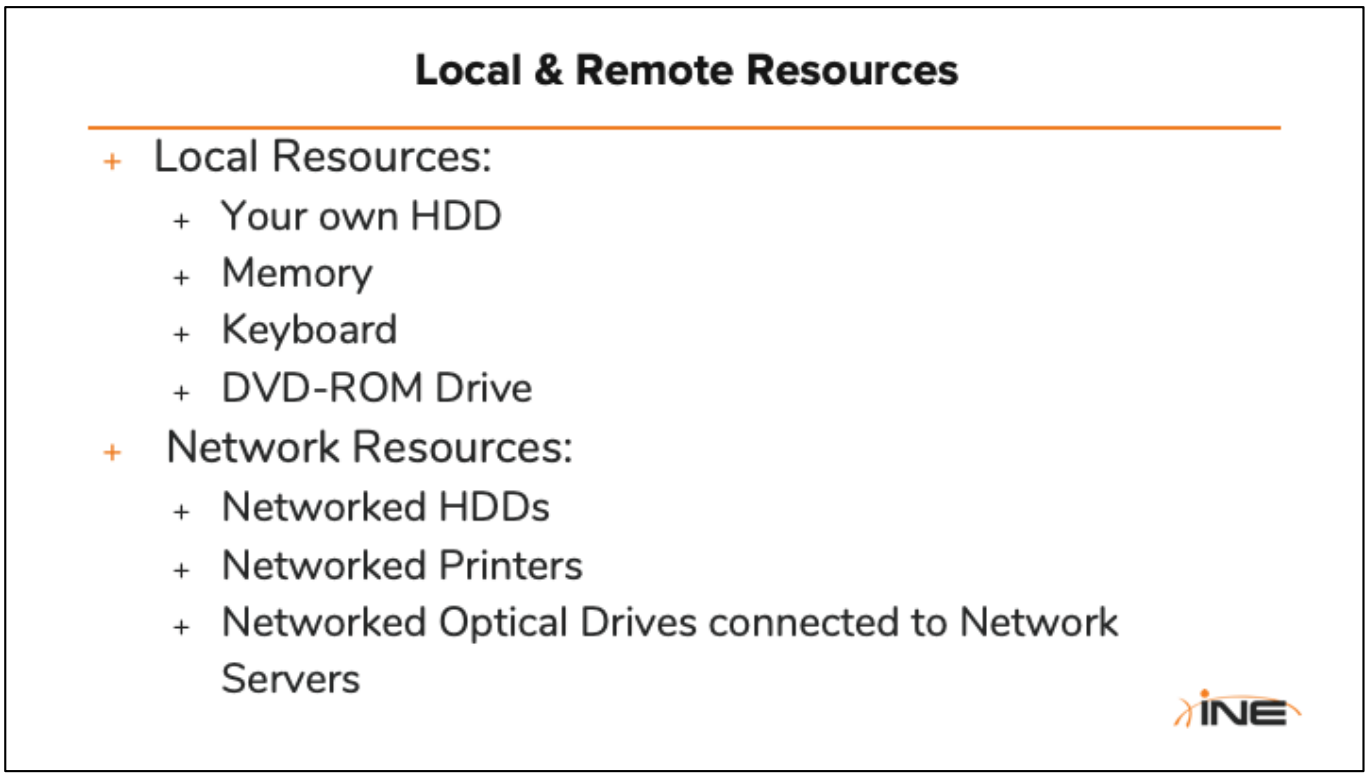
----Networked home devices (like DVRs)



NICs, Switches, Routers, Firewalls and IPS devices



Today, most of what we do on our laptops, PCs, tablets and smartphones requires pulling data from another device. Such as Retrieving a website, an online calendar, downloading music files and videos.
-

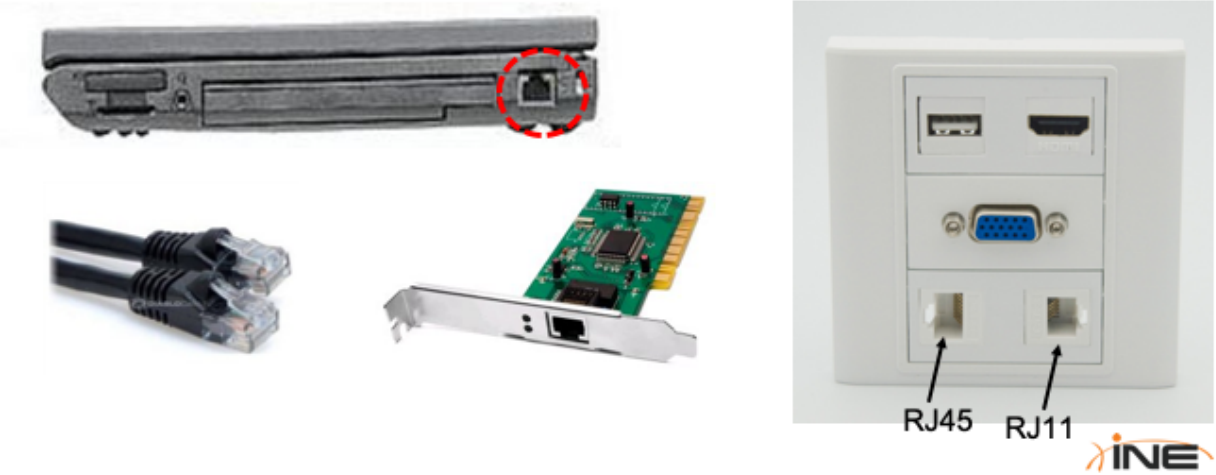


You can't tell just by looking at something if it is a LR or a NR. A printer sitting next to you could also be on the network.

In the past, networking consisted of accessing shared resources on the local network (shared printers, network drives, shared folders, etc) and also accessing the Internet (primarily for research or entertainment) Today, many tasks that used to utilize shared resources (such as Email, File Storage and Calendaring) now make use of Internet resources instead (Gmail, DropBox, Google Calendar).

Common Network Components - NICs

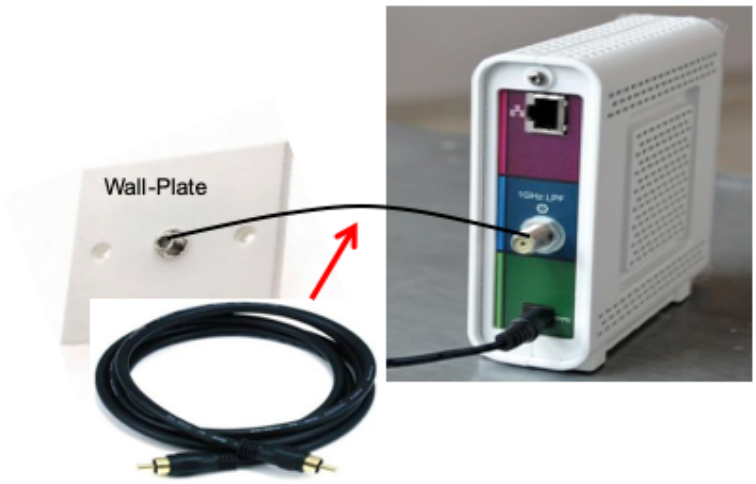
+ Network Interface Cards, Connectors and Cables



LAN / Ethernet NICs and cables on this page. Others on next page.

Common Network Components - NICs

+ Coaxial Cable NICs



Coaxial Cable

Connector type is called an SMA (SubMiniature version A) which come in Male and Female versions. There are other types of connectors as well.

Common Network Components - NICs

+ Wi-Fi NICs

Wi-Fi NICs are frequently built-in and can't be seen.

-

Guts of a Tablet (Nexus 7) are shown.

Common Components - Switches

+ Switches

Cisco Nexus 9508 start around $50k

Common Components - Routers

+ Routers

Cisco 2801 ISR

Externally a router may not look much different than a switch.
-
Talk about Hardware vs Software-based features. Routers are more SW-based and so can do more things.

Common Components – Firewalls & IPS

- Traditional Firewalls
  - Inspected only network address (IPv4/v6) and TCP/UDP port numbers
  - Based all forward-or-block decisions based off of those values
- Next-Generation Firewalls
  - Allow for deep-packet inspection
  - Ability to forward or block packet based on application awareness
  - Can utilize outside services to detect malicious attacks
- IPS = Intrusion Prevention System

Common Components – Firewalls & IPS

Firepower 9000 Series

Cisco ASA 5500-X

Topic Overview

- Common Wi-Fi Components
- Introduction To Cisco DNA Center

Common Components – Wi-Fi

- Wi-Fi Access Points

Common Components – Wi-Fi Controllers

- Controllers
  - Central point of management for groups of Access Points
  - Control Wi-Fi access for Clients
- Controller differentiators
  - Quantity of Wi-Fi Clients supported
  - Features available
  - Appliance or Cloud-based
  - Type & quantity of uplink interfaces

Many controllers also have integrated features such as Firewalls, ACLs and other security features.

The Cisco 9800 series WLAN controllers are shown here.

Components - Cisco DNA Center

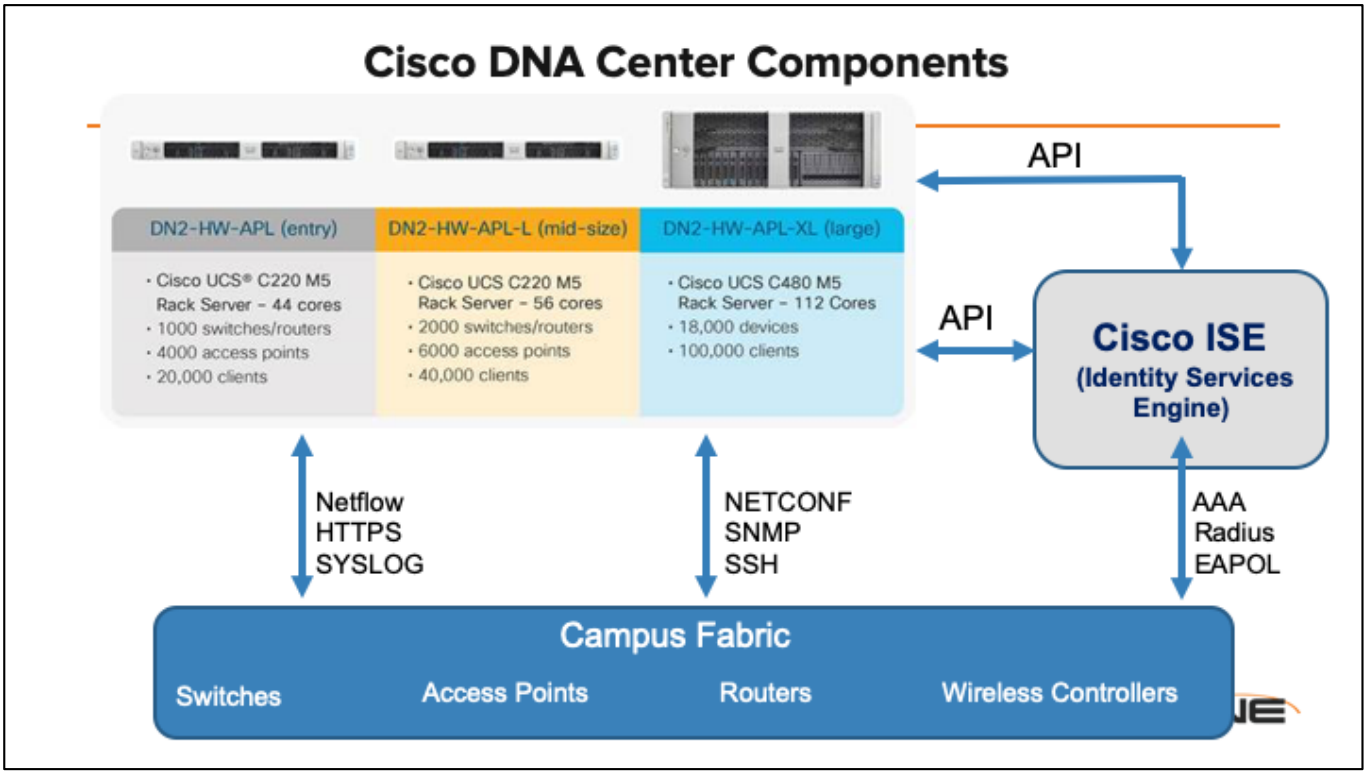
- DNA = Digital Network Architecture
- Cisco DNA Center is a centralized management dashboard for complete control of a network
- Provides a central automation and analytics platform to facilitate “Intent-Based Networking”

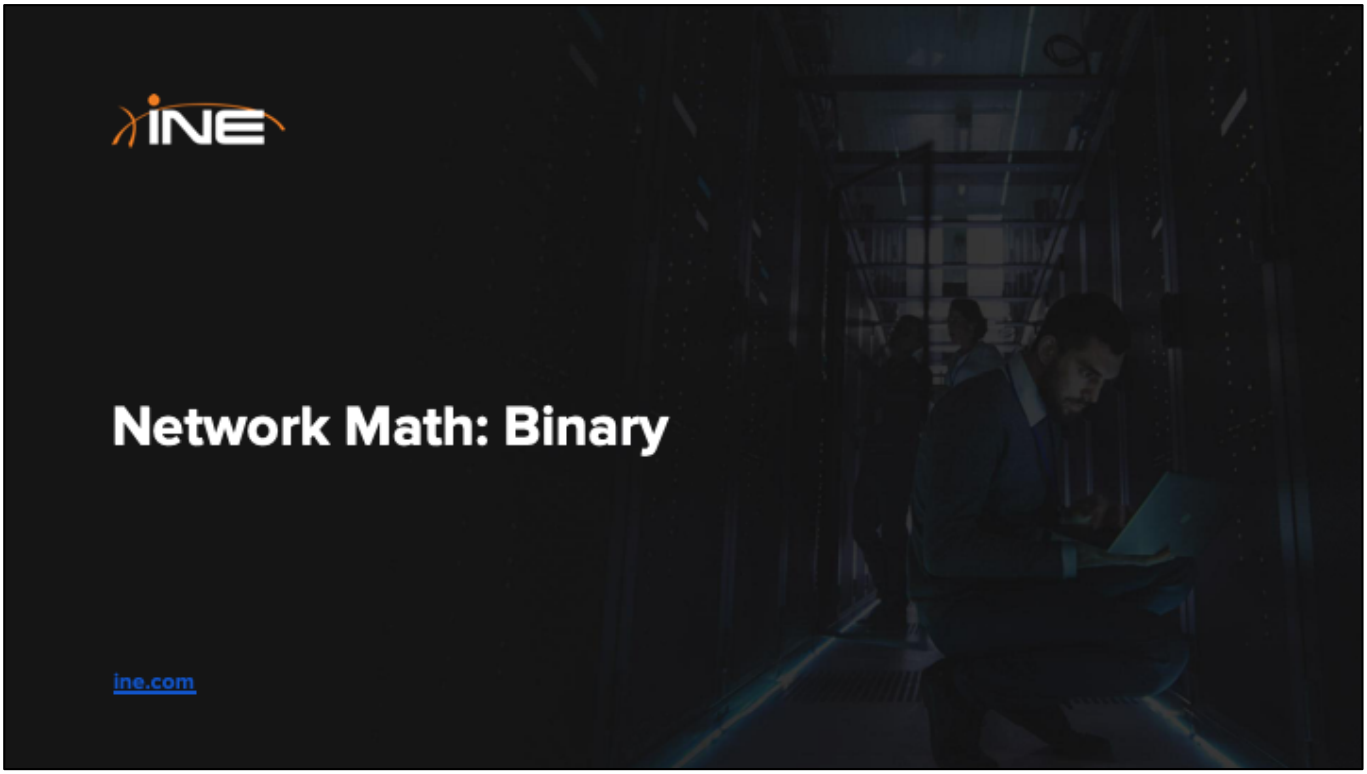
Intent based networking: a new approach to **networking**, where special software helps to plan, design and automatically implement on the fly changes to the **network**, improving its availability and agility.

The idea here is that before a single end-user or application touches your network, you have pre-planned how the network should respond to these things when they DO get connected. Your “intent” (what resources users should have access to, QoS policies for different applications, etc) is given to the Controller which then, in turn, translates that intent into usable configurations that are pushed down to network devices.

Cisco DNA Center

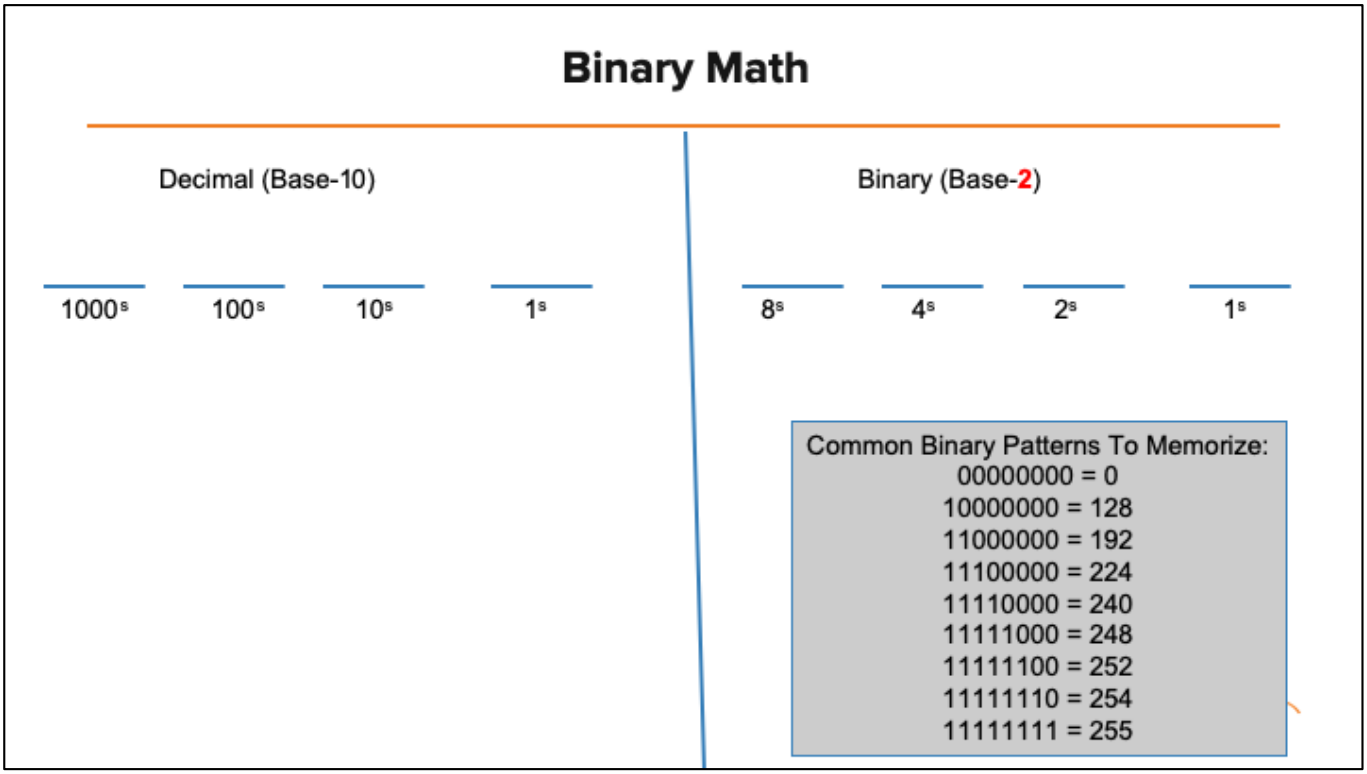
- Appliance pre-built with Cisco DNA Center software
- A controller and analytics platform
- Central point of GUI-based network control allowing:
  - Design your network
  - Create topology maps and diagrams
  - Identify/list "Golden Images" for software deployments
  - Create wireless profiles and SSIDs
  - GUI-based configuration of network devices



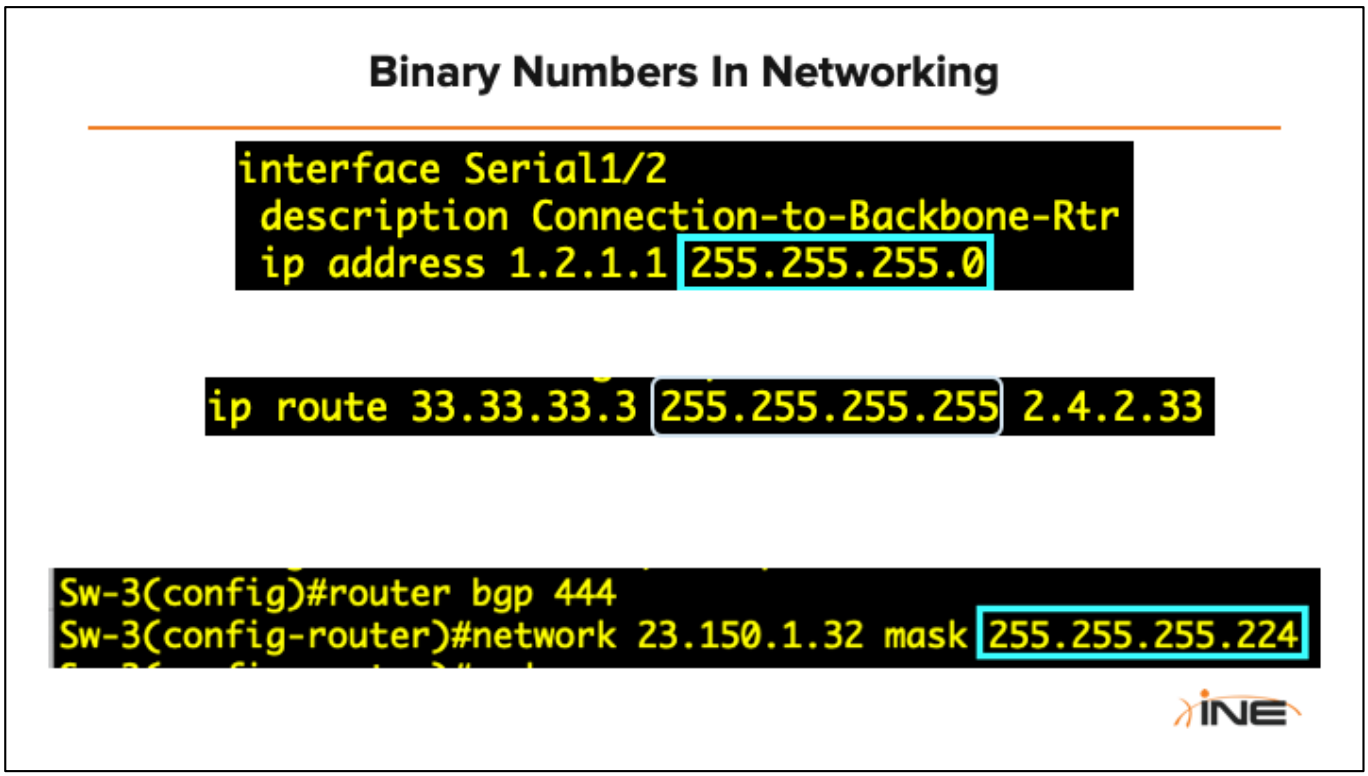


Topic Overview

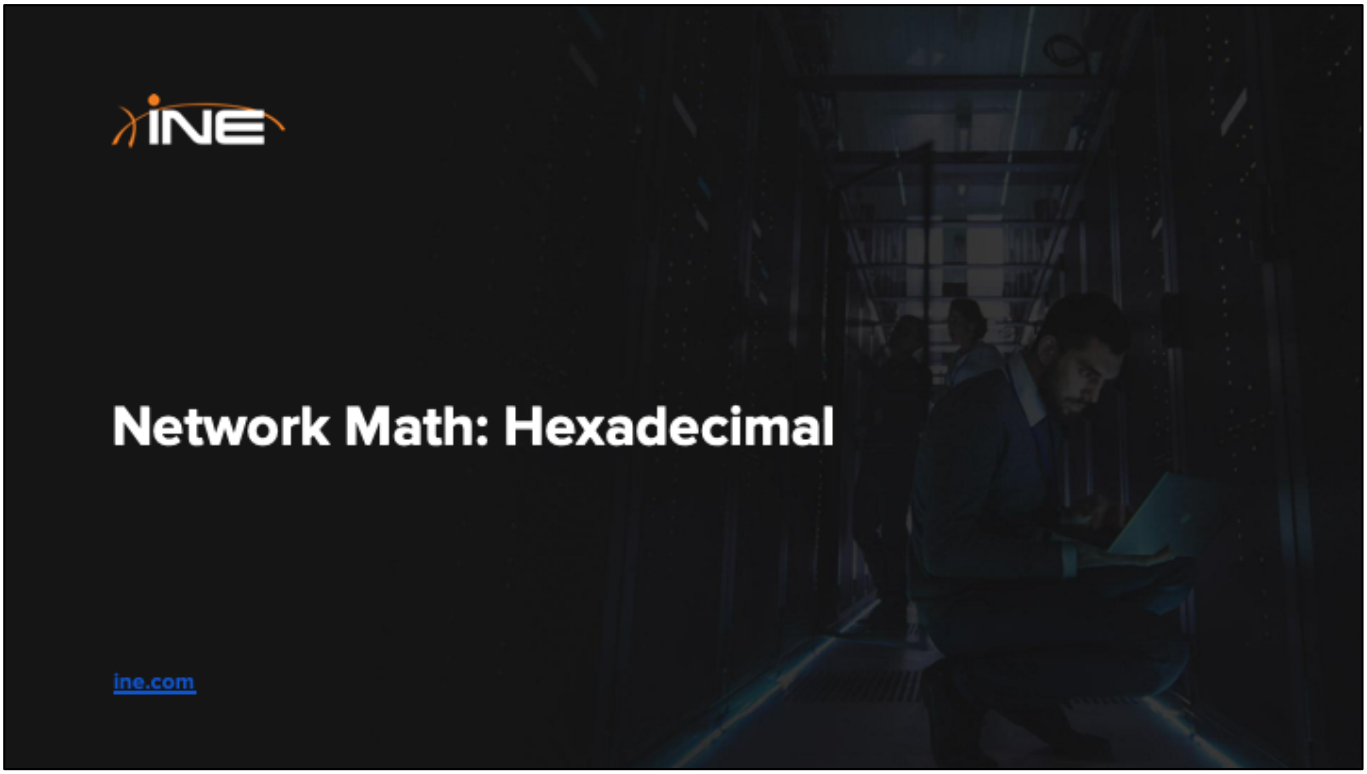
+ Introduction To Binary



Whiteboard each of these.

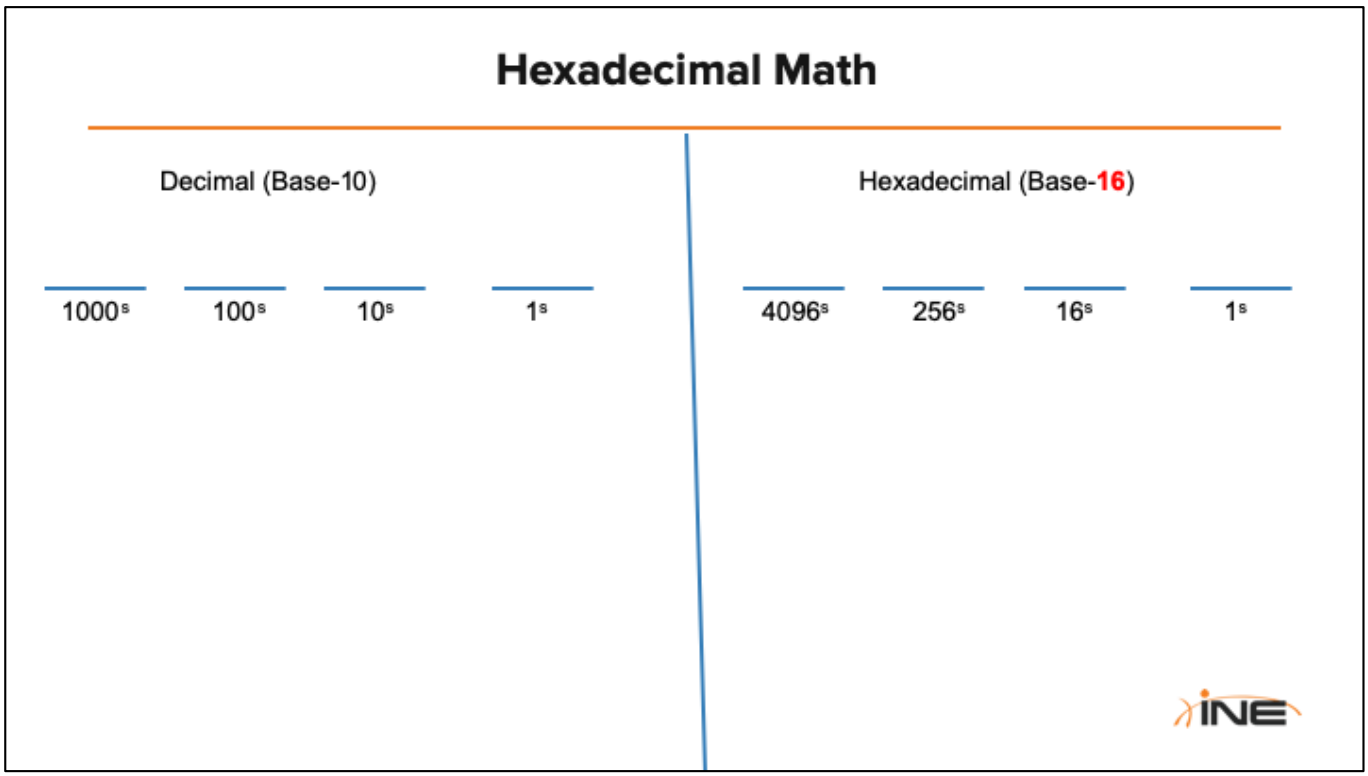


Whiteboard each of these.

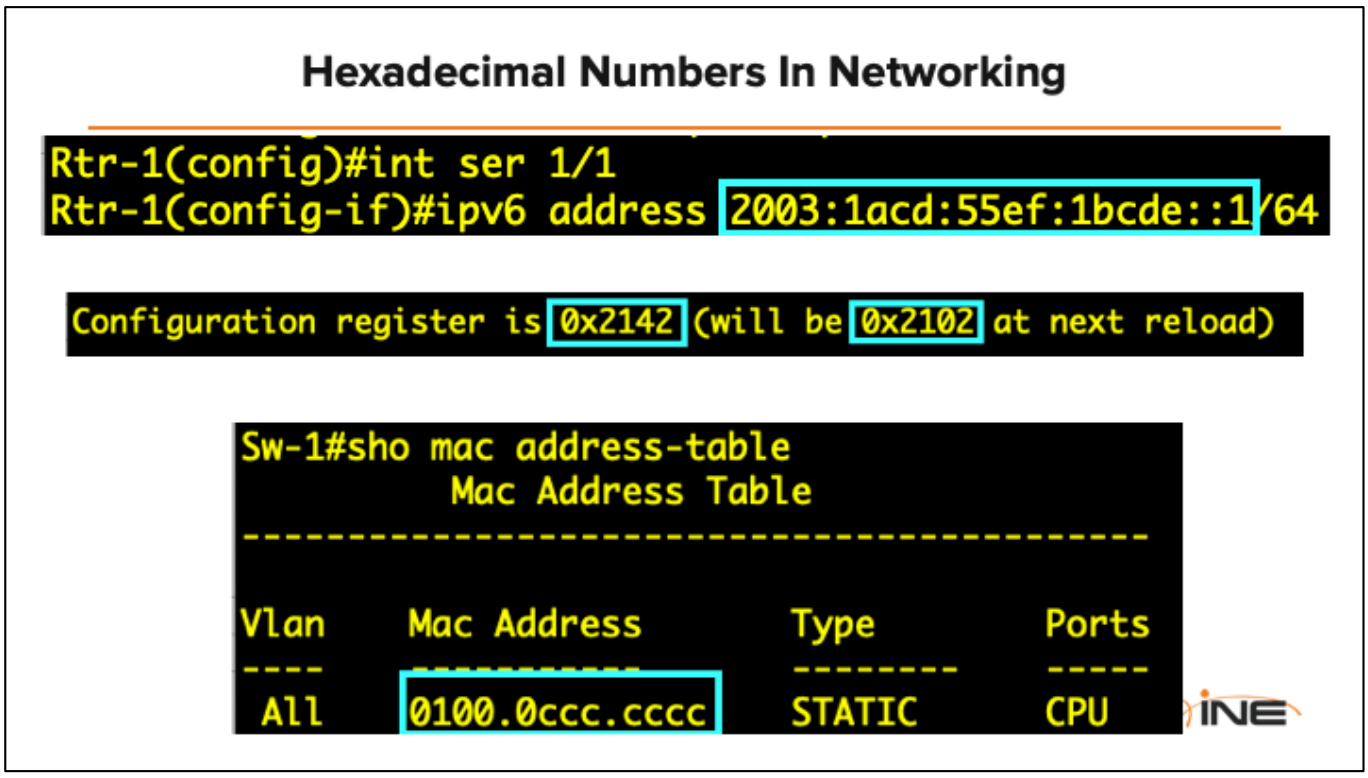


Topic Overview

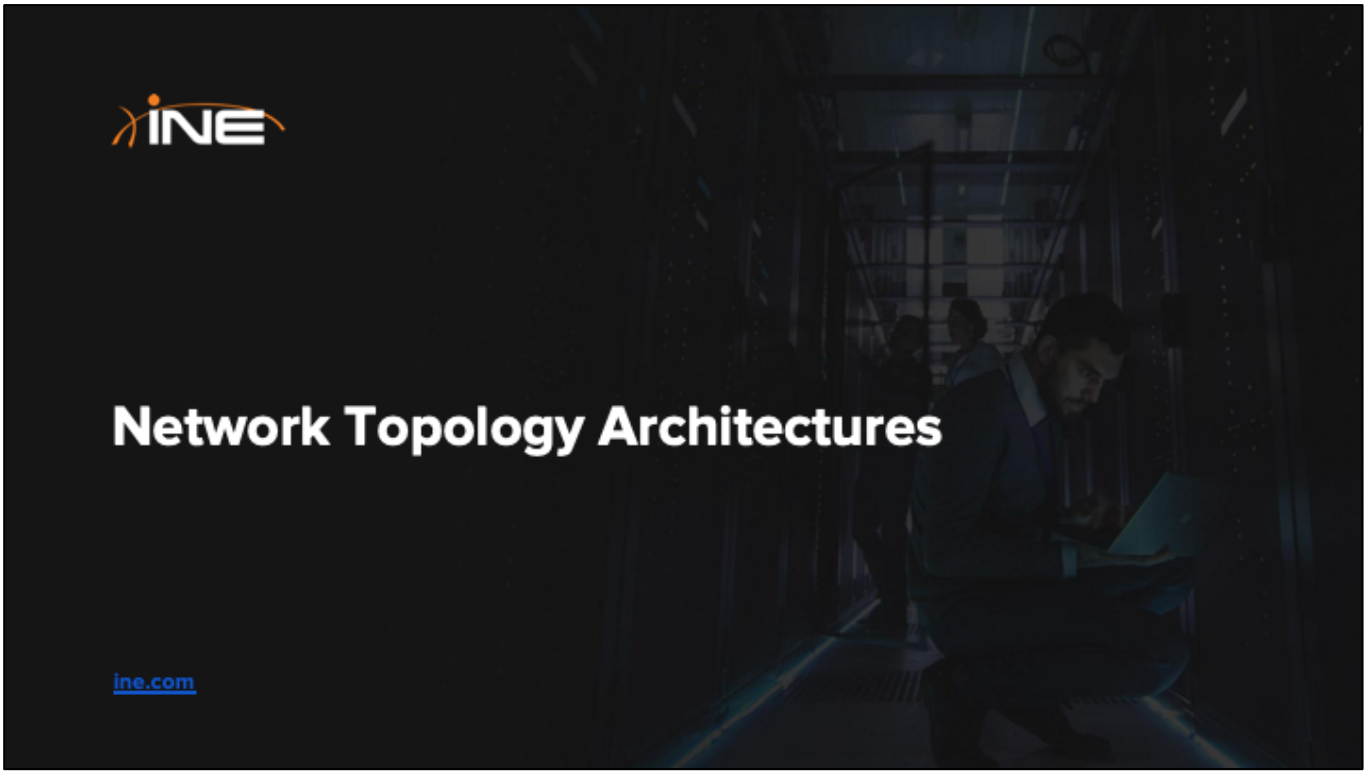
+ Introduction To Hexadecimal



Whiteboard each of these.



Whiteboard each of these.



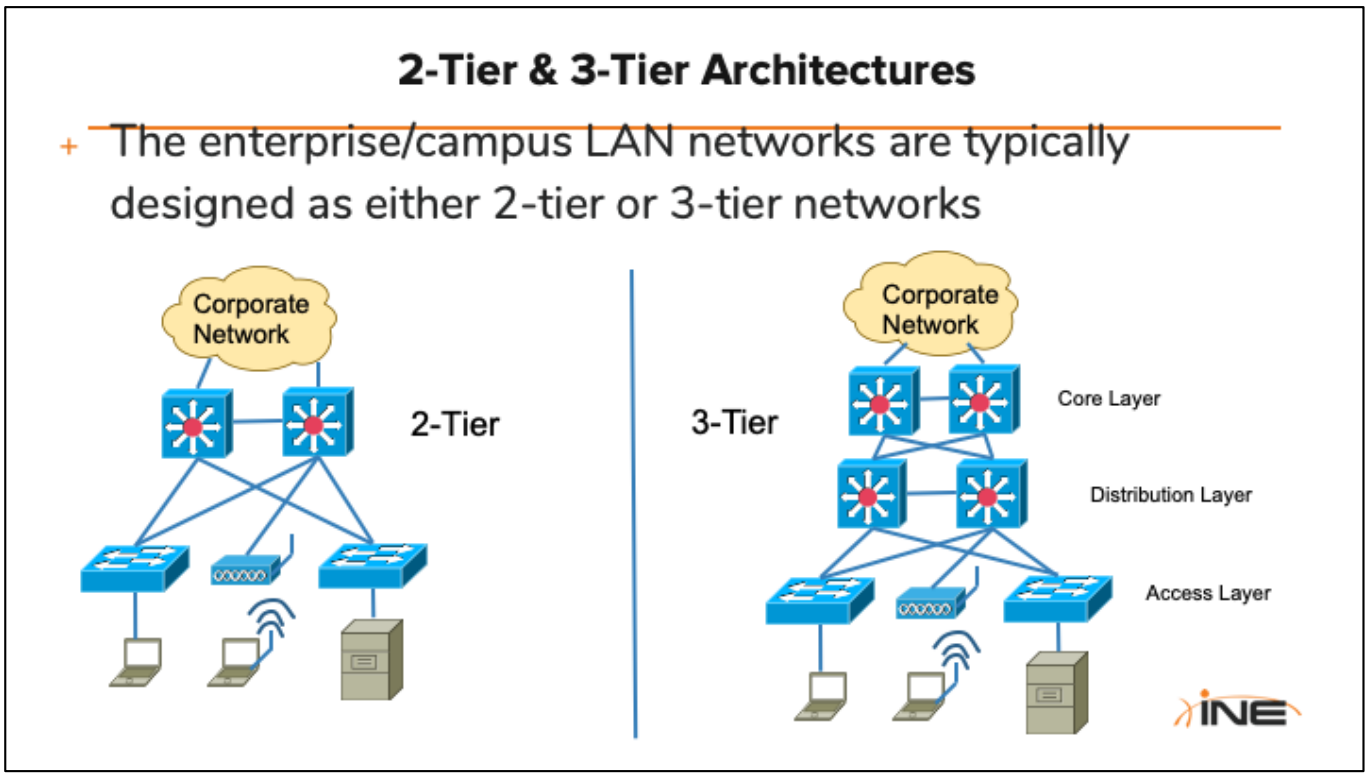
Topic Overview

+ 2-Tier & 3-Tier Architectures
+ Spine-Leaf Architectures
+ WAN Architectures
+ SOHO Architectures
+ On-Premise Vs. Cloud-Based Architectures

Network Topology Architectures

- Networks can be designed in a variety of ways
- Each of these ways (i.e. an Architecture) will dictate things such as:
  - Physical devices and cabling needed
  - Path of data traffic
  - Redundancy
  - Use of 3rd party services

Some architectures will require that you must utilize the services of a 3rd party such as an ISP or WAN Service Provider. The costs of implementing these services, planning for their failure, and accounting for any latency they might introduce must all be factored into your planning.



The 2-Tier network has also been called the “Collapsed Core” architecture.

Some of the characteristics of this type of architecture:
---Utilizes several different types of devices at the Access Layer in order to accommodate a wide variety of host devices (access points with multiple radios, switches with several kinds of interfaces).
---Implement access-layer security protocols to allow only authorized access to the network.
---Quick and easy connectivity to end-user devices is a primary concern

Spine-Leaf Architectures

- Data center networks are typically designed as Spine-Leaf architectures
- Interconnections between switches can be L2 or L3

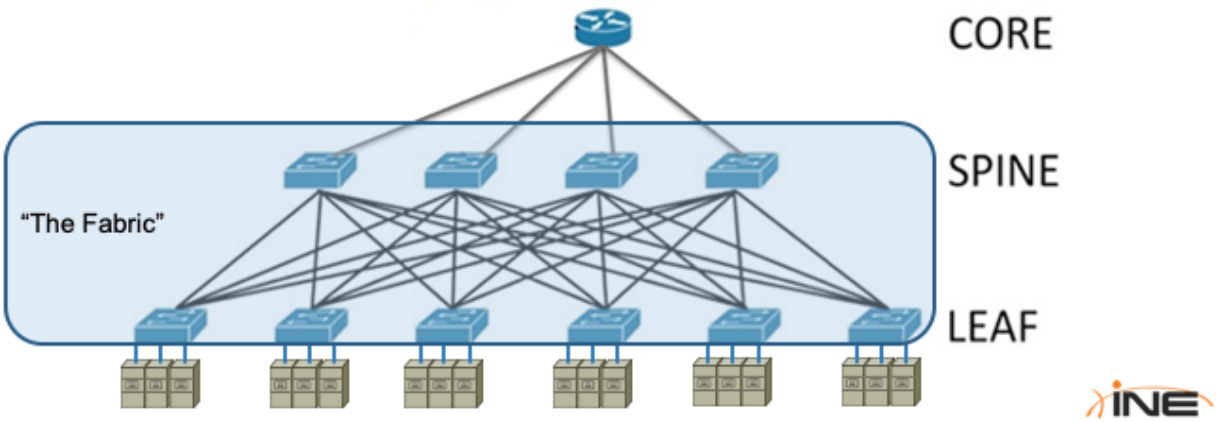
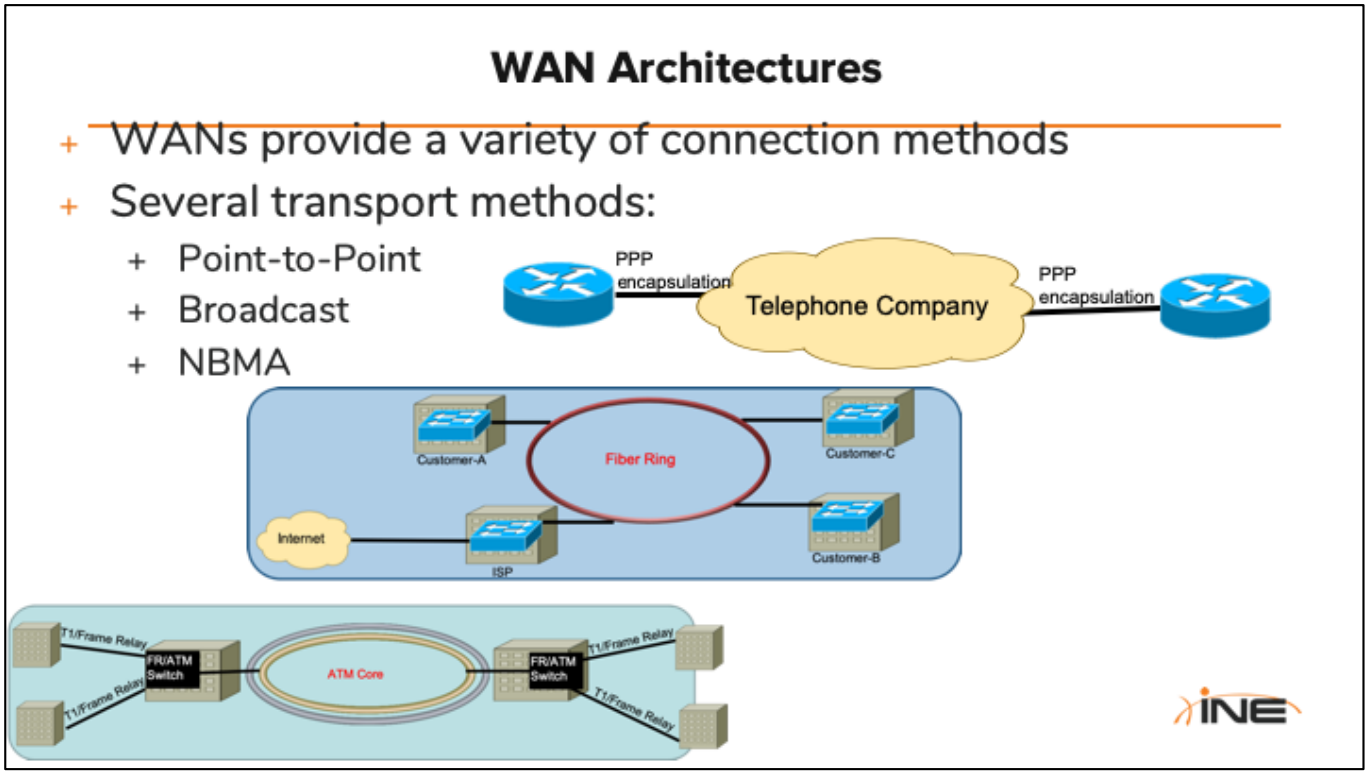


Image courtesy of searchdatacenter.techtarget.com

This type of architecture is best suited for data center traffic that is more likely to move east-to-west rather than north-to-south.

Typically connections between all switches will be Layer-3 in order to prevent bridging loops and the delays induced by using Spanning-Tree (or other similar loop-prevention technologies).

Some of the characteristics of this type of architecture:
---Utilizes the highest speed links possible between devices (10Gbps and up)
---Resiliency and redundancy are a major factor. These types of networks are designed to almost NEVER go down.
---The switches used here are more expensive than your typical Enterprise/Campus switches because they utilize higher-speed connections, and have many redundant hw/sw features built-in



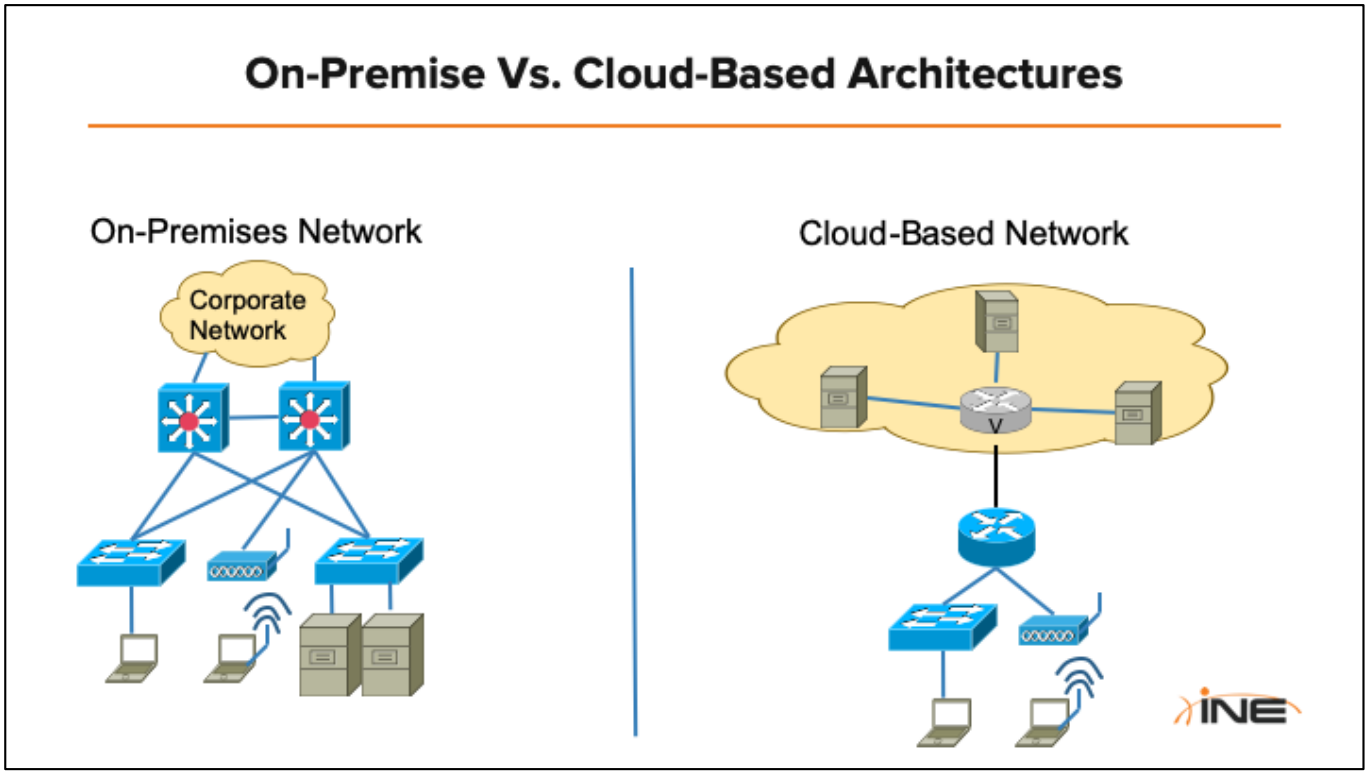
Some of the characteristics of this type of architecture:
---Available bandwidth is much less than Enterprise LAN bandwidth
---This network is out of your control. You can't monitor it, view its health or fix it when it goes down.
---Almost always the actual cables that are transporting your data are also used to transport data from other customers as well.
---Privacy of your data as it traverses these types of network is a major concern.

SOHO Architectures

- SOHO = Small Office / Home Office
  - Less equipment demands
  - Less need for authentication and security
  - Difficult to manage and enforce policy from HQ

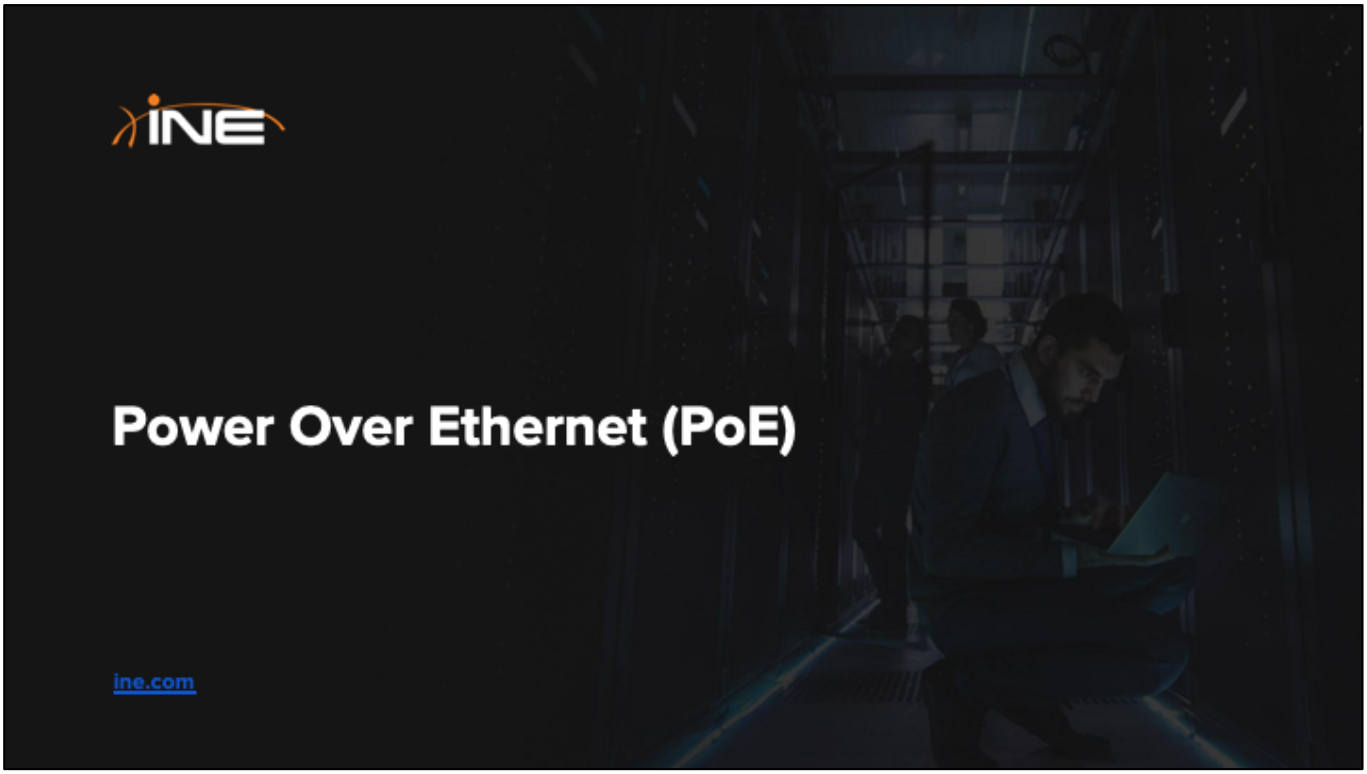
Small Office Network

Home Office Network



On-premises characteristics:
-----Majority (if not all) of resources that end-users need physically reside within the enterprise.
-----The network admin has control (and responsibility) for end-to-end reachability between end-users and the resources they need.
-----An almost endless supply of options available for controlling the network and security implementations.

Cloud-based characteristics:
----Responsibility for cloud-based resource uptime shifted to cloud-provider
----From the perspective of the customer, choices are very limited with regards to cloud network segmentation and security.
----Confidentiality of data sent to/from the cloud a major concern

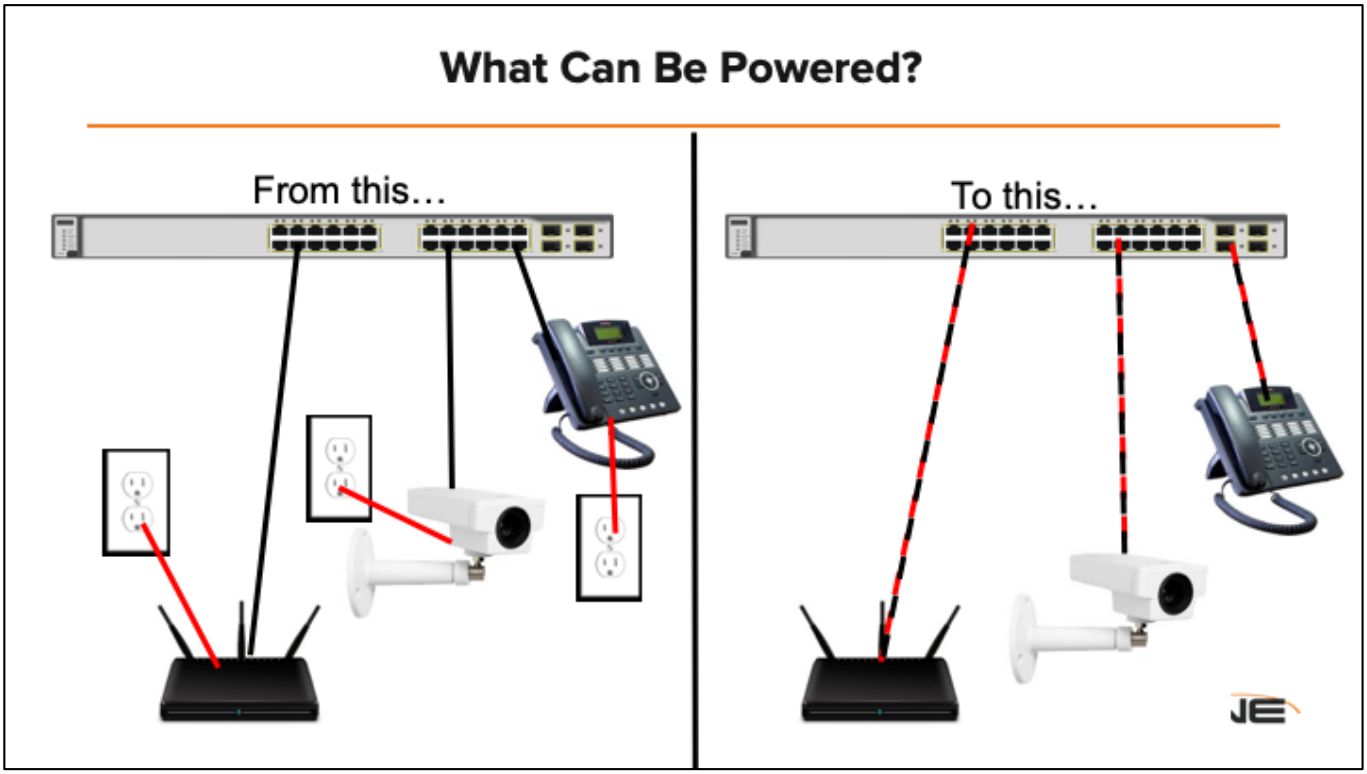


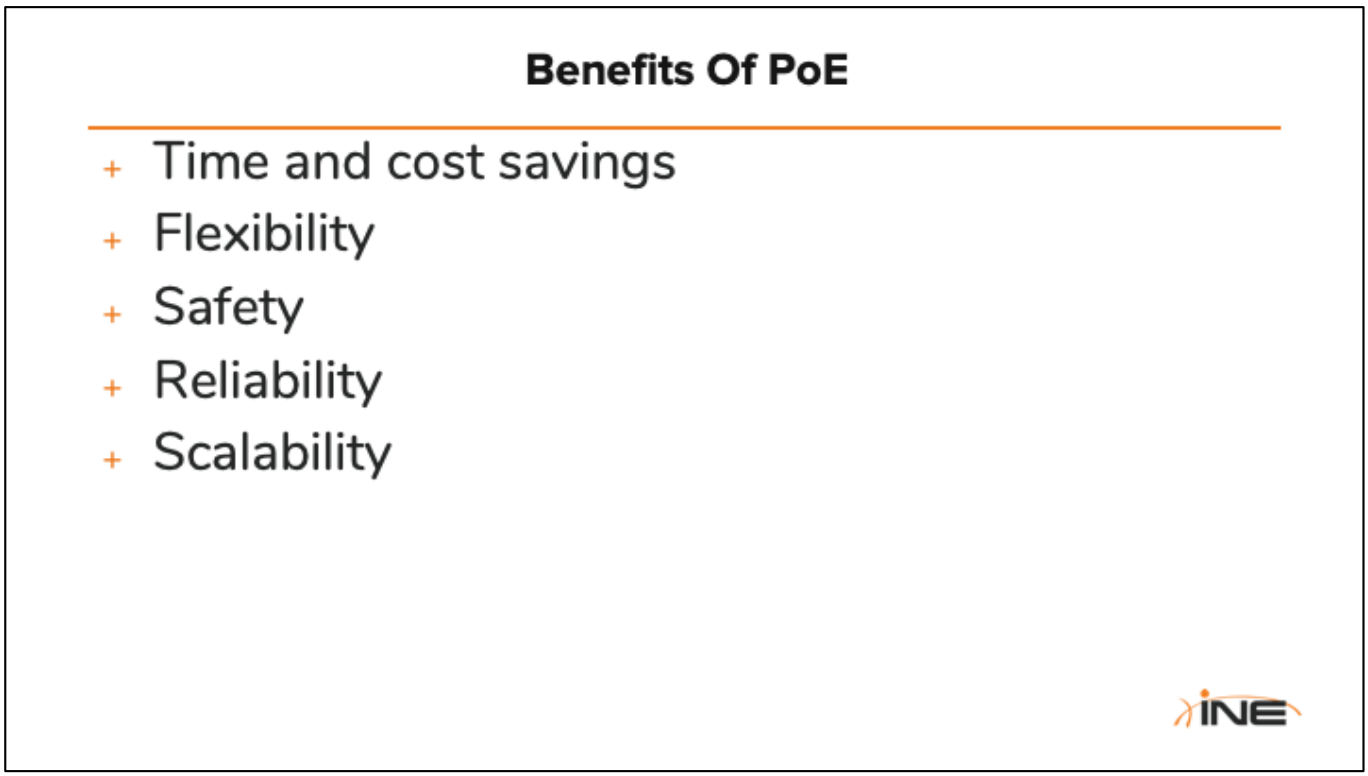
Topic Overview

- Why Do We Need PoE?
- What Can Be Powered?
- Benefits Of PoE
- PSE & PD Defined
- How Much Power Can Be Sent?
- How Is Power Delivered?
- PoE Detection & Negotiation
- PoE Monitoring

Why Do We Need PoE?

- All host devices that connect to a network require power
  - Laptops
  - PCs
  - Printers
  - IP Phones
  - IoT devices
- Finding available AC connections for all of these devices can be difficult
- PoE allows us to provide power to these devices directly from the network switch





Time and cost: Less cables have to be run through walls, around cabinets, into ceilings, etc.

Flexibility: Now, if you can run an Ethernet cable to a location you can also run power to that same location.

Safety: POE delivery is intelligent, and designed to protect network equipment from overload, underpowering, or incorrect installation.

Reliability: POE power comes from a central and universally compatible source, rather than a collection of distributed wall adapters. Without PoE you have to be concerned with obtaining a power cable that has the correct pinouts and plugs for your particular country. And what if you want to move that device to a different country? By using PoE you don't have to worry about that. Also, PoE power-supplying-equipment can be backed-up by an uninterruptible power supply, or controlled to easily disable or reset devices.

Scalability: You don't have to worry about being limited to only a handful of power outlets in a room. With a PoE switch in that room you now have dozens of connections that can provide power.

PSE & PD

- Standards-based PoE relies on the IEEE 802.3af, 802.3at and 802.3bt standards
- PoE devices categorized as:
  - PSE – Power Sourcing Equipment
  - PDs – Powered Devices
- PSEs are typically network switches or power injectors

Shown here are some examples of PoE injectors. You would use these when you have a PD that is ONLY capable of being powered by PoE but your network switch doesn't support PoE. In this case, you're not really reaping any benefits from PoE because you still need to plug a PoE injector into an AC outlet.

How Much Power Can I Get?

IEEE Standard	Type	Power Budge per Device
IEEE 802.3af	Type 1	15.4W
IEEE 803.2at / PoE+	Type 2	30.8W
802.3bt / Cisco UPoE	Type 3	60W
IEEE 802.3bt / UPoE+	Type 4	90-95W

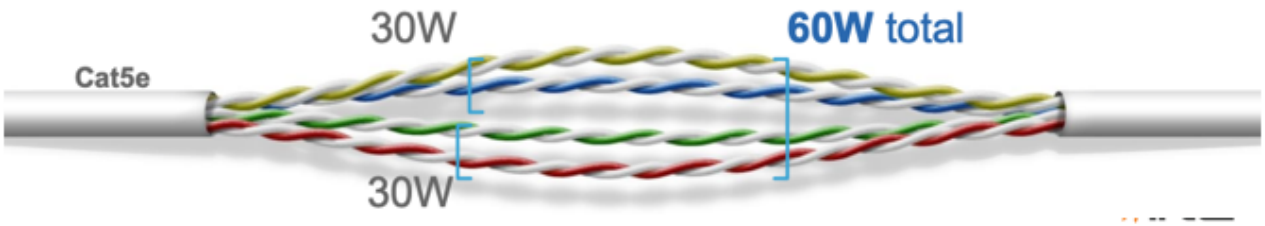
Here you can see that there are various PoE standards. Depending on whichever standard(s) your PSE supports will dictate the maximum power that device can deliver.

UPoE stands for “Universal Power Over Ethernet”.

Keep in mind that each type of switch that can provide power has something called a “Power Budget” which is the TOTAL amount of power that can be delivered via PoE. Many switches do not have the capability to deliver maximum PoE levels across each and every switchport.

How Is Power Delivered?

- Ethernet cables contain four pairs of twisted cables (8-wires total)
- IEEE 802.3af and 802.3at standards utilize two of these pairs (4-wires) to deliver power
- Cisco UPoE and UPoE+ utilize all 8-pairs to deliver power



The graphic shown here demonstrates how UPoE delivers 60W over Category5e twisted pair ethernet cable.

There is an IEEE equivalent to Cisco's UPoE which is called IEEE 802.3bt (also called 4PPoE). This is also capable of delivering up to 90W of power by using all four pairs of UTP cabling to deliver power.

PoE Detection & Negotiation

- PoE uses a detection technique to determine if:
  - PSE is connected to a PD or not
  - How much power the PD requires
- General summary of initial steps
  - PSE outputs a small amount of power to detect if there is any resistance
  - PDs have a special resistor in the NIC that will respond, and limit this incoming voltage and reflect back a certain amount to PSE
  - PSE now knows it is connected to a PD and, depending on the current/voltage it receives back, performs this step a few more times to detect the type-and-classification of PD
  - PSE finally knows just how much power to deliver

Further steps for power negotiation
----After PD is receiving the minimum power it needs, it can send a LLDP or CDP message to PSE
----LLD-MED option is used to indicate the actual amount of power the PD requires
----CDP can also be used for this same purpose

Monitoring PoE On Cisco Devices

```
Stack-1# show cdp neighbor detail
-------------------------
Device ID: SEP001121116D78
Entry address(es): IP address: 192.168.1.249
Platform: Cisco IP Phone 7970,  Capabilities: Host Phone
Interface: GigabitEthernet1/0/2,  Port ID (outgoing port): Port 1
Holdtime : 150 sec
Version :  SCCP70.8-0-0-74S
advertisement version: 2
Duplex: full
Power drawn: 10.250 Watts
Power request id: 28024, Power management id: 3
Power request levels are:10250 6300 0 0 0
```

Image courtesy of cisco.com

In this output the “Power Drawn” represents the maximum required power for this phone, which is 10250 milliwatts (10.25 W)
However this phone has also advertised that is capable of operating with reduced screen brightness at 6.3 W

Monitoring PoE On Cisco Devices

```
Stack-1# show power inline
Module   Available     Used     Remaining
(Watts)    (Watts)    (Watts)
------   ---------   --------   ---------
1            420.0       22.2       397.8
2            370.0       18.2       351.8

Interface Admin  Oper       Power   Device              Class Max
                            (Watts)
--------- ------ ---------- ------- ------------------- ----- ----
Gi1/0/1   auto   on         6.3     IP Phone 7960       0     15.4
Gi1/0/2   auto   on         10.3    IP Phone 7970       3     15.4
Gi2/0/1   auto   on         15.4    IP Phone CP-7970G   3     15.4
Gi2/0/2   auto   on         8.5     AIR-AP1220-IOS      n/a   15.4
```

Image courtesy of cisco.com

The output of this command shows the total power budget (total power available to be delivered) by each switch in this switch stack (grouping of switches) and how much has been consumed so far.