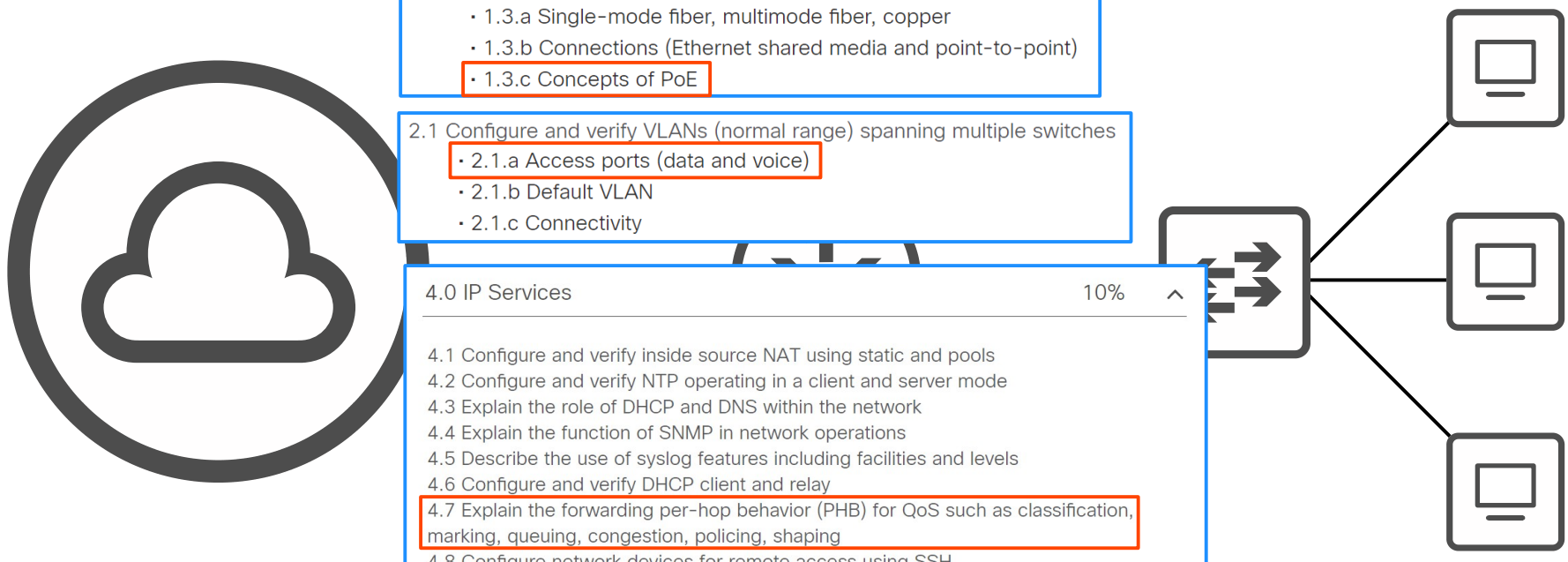
JEREMY'S IT LAB

CCNA Day 46

Quality of Service (Part 1)

1.3 Compare physical interface and cabling types
- 1.3.a Single-mode fiber, multimode fiber, copper
- 1.3.b Connections (Ethernet shared media and point-to-point)
- 1.3.c Concepts of PoE

2.1 Configure and verify VLANs (normal range) spanning multiple switches
- 2.1.a Access ports (data and voice)
- 2.1.b Default VLAN
- 2.1.c Connectivity



4.0 IP Services 10%

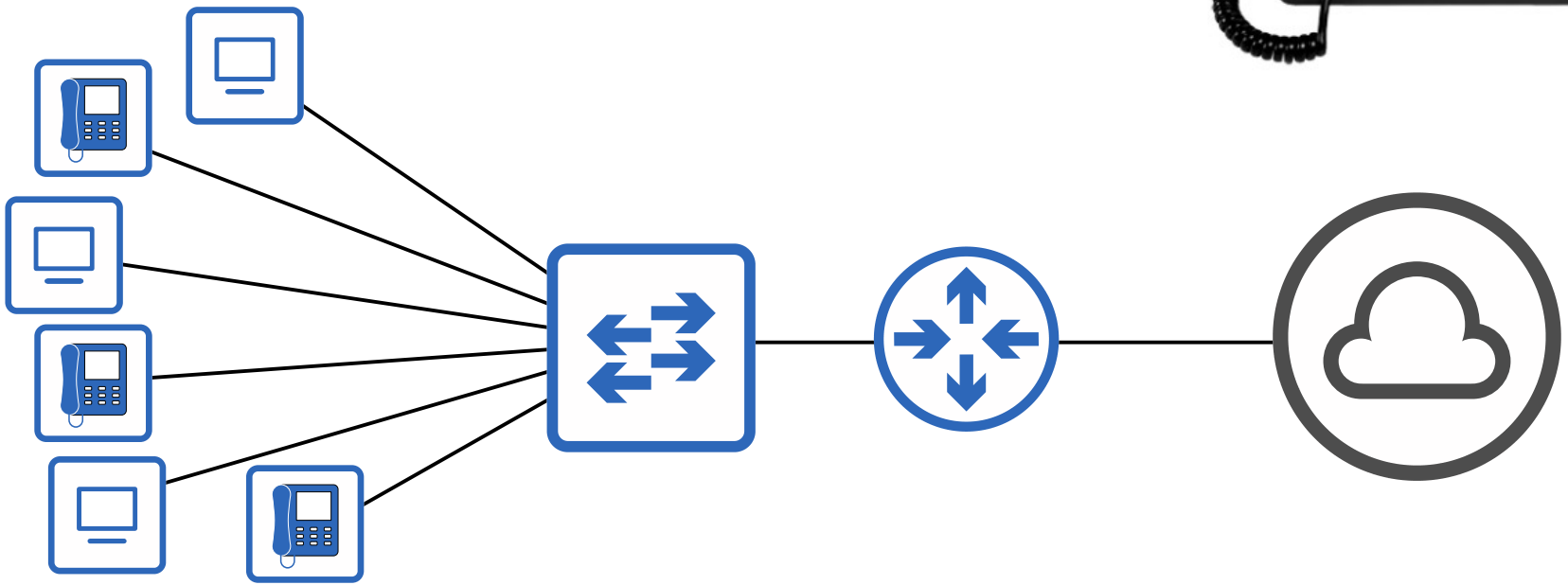
4.1 Configure and verify inside source NAT using static and pools
4.2 Configure and verify NTP operating in a client and server mode
4.3 Explain the role of DHCP and DNS within the network
4.4 Explain the function of SNMP in network operations
4.5 Describe the use of syslog features including facilities and levels
4.6 Configure and verify DHCP client and relay
4.7 Explain the forwarding per-hop behavior (PHB) for QoS such as classification, marking, queuing, congestion, policing, shaping
4.8 Configure network devices for remote access using SSH
4.9 Describe the capabilities and function of TFTP/FTP in the network

Things we'll cover

- IP Phones/Voice VLANs
- Power over Ethernet (PoE)
- Intro to Quality of Service (QoS)

IP Phones

- Traditional phones operate over the *public switched telephone network* (PSTN).
- Sometimes this is called POTS (Plain Old Telephone Service).
- IP phones use VoIP (Voice over IP) technologies to enable phone calls over an IP network, such as the Internet.
- IP phones are connected to a switch just like any other end host.

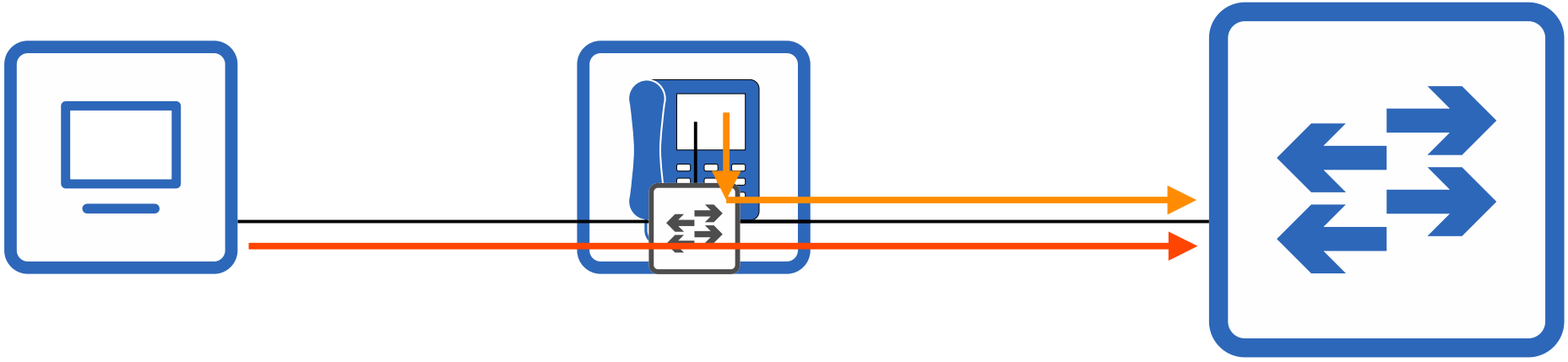


IP Phones

- IP phones have an internal 3-port switch.
  → 1 port is the ‘uplink’ to the external switch.
  → 1 port is the ‘downlink’ to the PC.
  → 1 port connects internally to the phone itself.

- This allows the PC and the IP phone to share a single switch port. Traffic from the PC passes through the IP phone to the switch.

- It is recommended to separate ‘voice’ traffic (from the IP phone) and ‘data’ traffic (from the PC) by placing them in separate VLANs.
  → This can be accomplished using a *voice VLAN*
  → Traffic from the PC will be untagged, but traffic from the phone will be tagged with a VLAN ID



IP Phones / Voice VLAN

```
SW1(config)#interface gigabitethernet0/0
SW1(config-if)#switchport mode access
SW1(config-if)#switchport access vlan 10
SW1(config-if)#switchport voice vlan 11

SW1#show interfaces g0/0 switchport
Name: Gi0/0
Switchport: Enabled
Administrative Mode: static access
Operational Mode: static access
Administrative Trunking Encapsulation: negoti
Operational Trunking Encapsulation: native
Negotiation of Trunking: Off
Access Mode VLAN: 10 (VLAN0010)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
Voice VLAN: 11 (VLAN0011)
![output omitted]
```

PC1 will send traffic untagged, as normal. SW1 will use CDP to tell PH1 to tag PH1's traffic in VLAN 11.

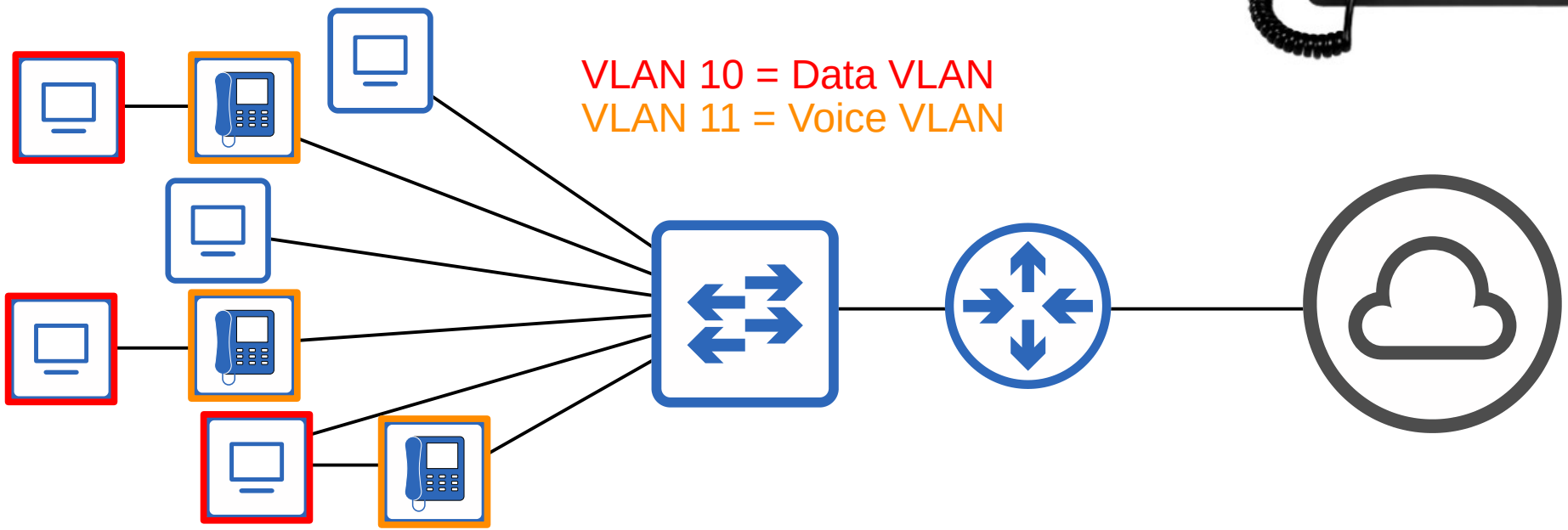
Although the interface sends/receives traffic from two VLANs, it is not considered a trunk port. It is considered an access port.

IP Phones / Voice VLAN

```
SW1#show interfaces trunk
SW1#
SW1#show interfaces g0/0 trunk

Port        Mode             Encapsulation  Status        Native vlan
Gi0/0       off              negotiate      not-trunking  1

Port        Vlans allowed on trunk
Gi0/0       10-11

Port        Vlans allowed and active in management domain
Gi0/0       10-11

Port        Vlans in spanning tree forwarding state and not pruned
Gi0/0       10-11
```

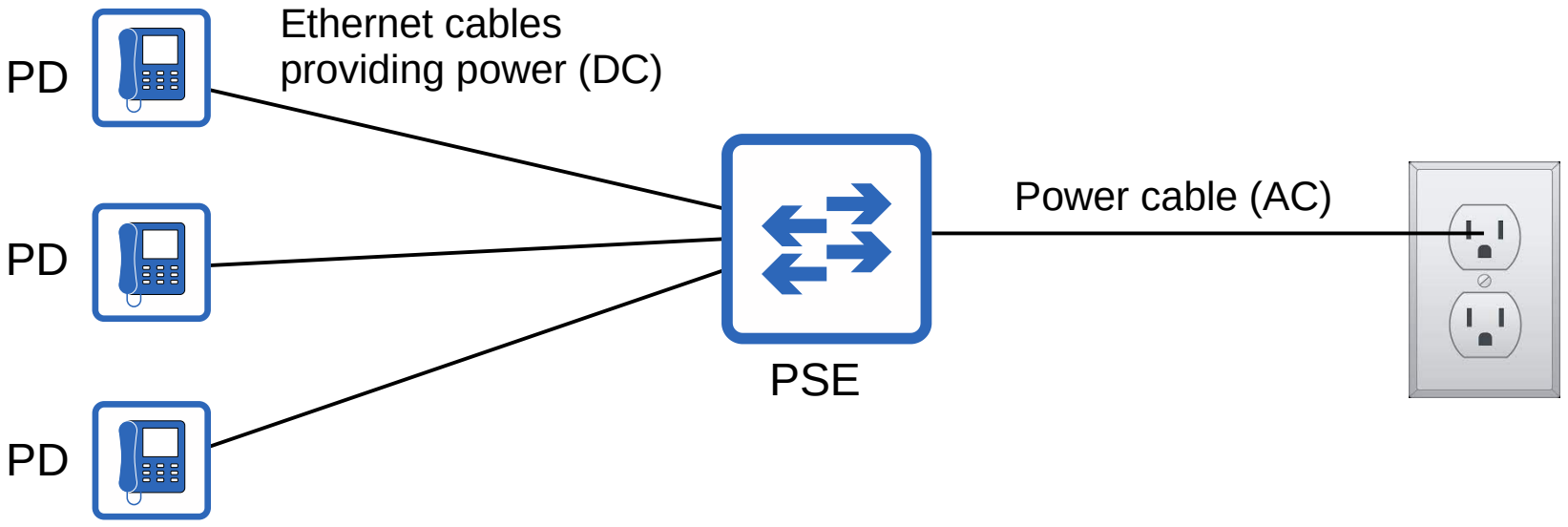
IP Phones

- Traditional phones operate over the *public switched telephone network* (PSTN).
- Sometimes this is called POTS (Plain Old Telephone Service).
- IP phones use VoIP (Voice over IP) technologies to enable phone calls over an IP network, such as the Internet.
- IP phones are connected to a switch just like any other end host.



Power over Ethernet (PoE)

- PoE allows Power Sourcing Equipment (PSE) to provide power to Powered Devices (PD) over an Ethernet cable.
- Typically the PSE is a switch and the PDs are IP phones, IP cameras, wireless access points, etc.
- The PSE receives AC power from the outlet, converts it to DC power, and supplies that DC power to the PDs.



Power over Ethernet (PoE)

- Too much electrical current can damage electrical devices.
- PoE has a process to determine if a connected device needs power, and how much power it needs.

  → When a device is connected to a PoE-enabled port, the PSE (switch) sends low power signals, monitors the response, and determines how much power the PD needs.

  → If the device needs power, the PSE supplies the power to allow the PD to boot.

  → The PSE continues to monitor the PD and supply the required amount of power (but not too much!)

- *Power policing* can be configured to prevent a PD from taking too much power.

  → **`power inline police`** configures power policing with the default settings: disable the port and send a Syslog message if a PD draws too much power.
    → equivalent to **`power inline police action errdisable`**
    → the interface will be put in an 'error-disabled' state and can be re-enabled with **`shutdown`** followed by **`no shutdown.`**

  → **`power inline police action log`** does not shut down the interface if the PD draws too much power. It will restart the interface and send a Syslog message.

Power over Ethernet (PoE)

```
SW1# conf t
Enter configuration commands, one per line. End with CNTL/Z.
SW1(config)# int g0/0
SW1(config-if)# power inline police
SW1(config-if)# end
SW1# show power inline police g0/0
Available:800(w) Used:32(w) Remaining:768(w)
Interface Admin  Oper       Admin      Oper       Cutoff Oper
          State  State      Police     Police     Power  Power
--------- ------ ---------- ---------- ---------- ------ -----
Gi2/1     auto   on         errdisable ok          17.2  16.7
```

Power over Ethernet (PoE)

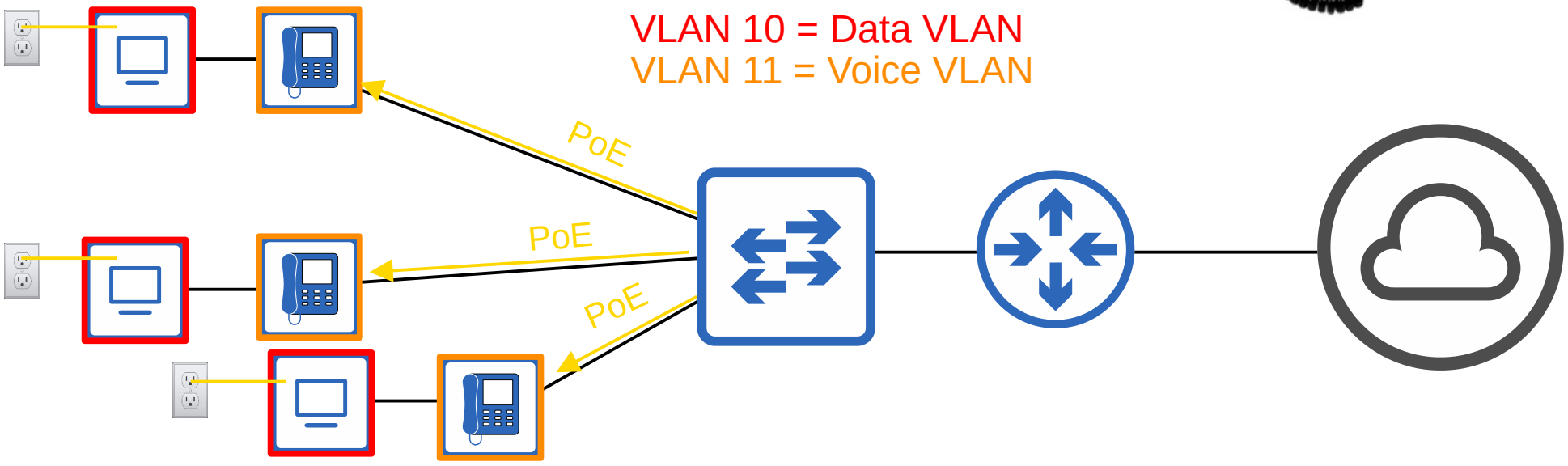
```
SW1# conf t
Enter configuration commands, one per line. End with CNTL/Z.
SW1(config)# int g0/0
SW1(config-if)# power inline police action log
SW1(config-if)# end
SW1# show power inline police g0/0
Available:800(w) Used:32(w) Remaining:768(w)
Interface Admin  Oper       Admin      Oper       Cutoff Oper
          State  State      Police     Police     Power  Power
--------- ------ ---------- ---------- ---------- ------ -----
Gi0/0     auto   on         log        ok          17.2  16.7
```

Power over Ethernet (PoE)

Name	Standard #	Watts	Powered Wire Pairs
Cisco Inline Power (ILP)	Made by Cisco, not standard	7	2
PoE (Type 1)	802.3af	15	2
PoE+ (Type 2)	802.3at	30	2
UPoE (Type 3)	802.3bt	60	4
UPoE+ (Type 4)	802.3bt	100	4

IP Phones

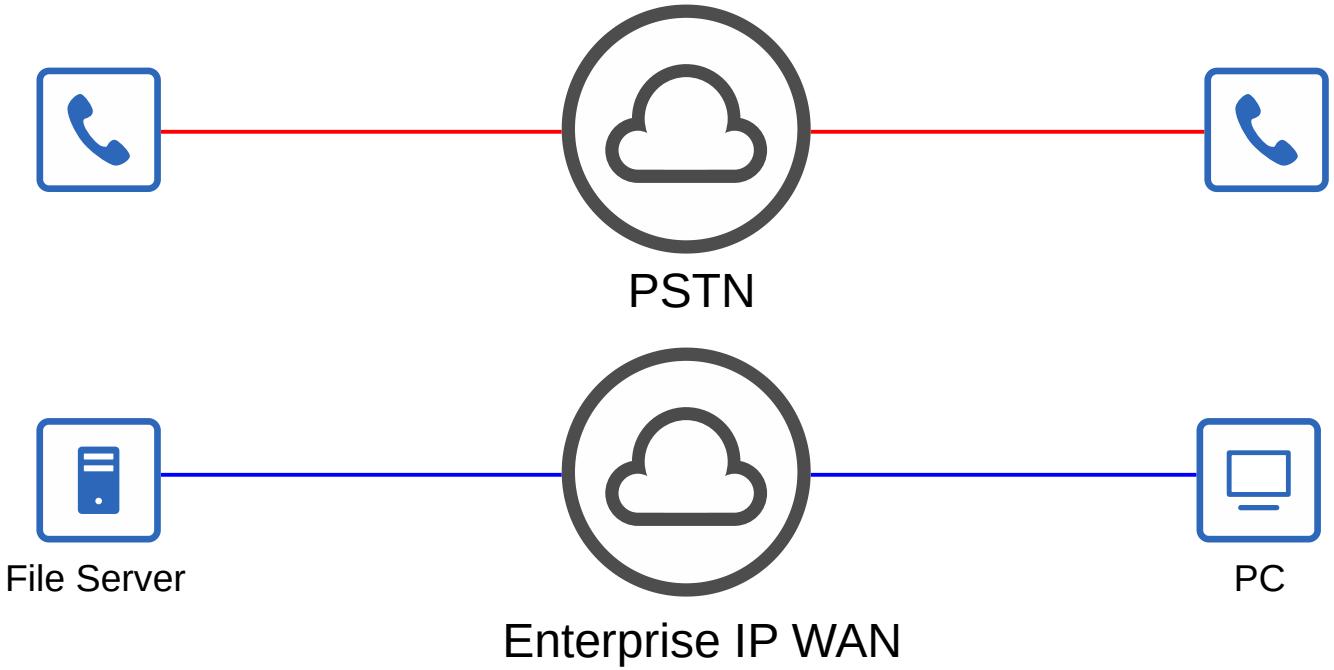
- Traditional phones operate over the *public switched telephone network* (PSTN).
- Sometimes this is called POTS (Plain Old Telephone Service).
- IP phones use VoIP (Voice over IP) technologies to enable phone calls over an IP network, such as the Internet.
- IP phones are connected to a switch just like any other end host.



Quality of Service (QoS)

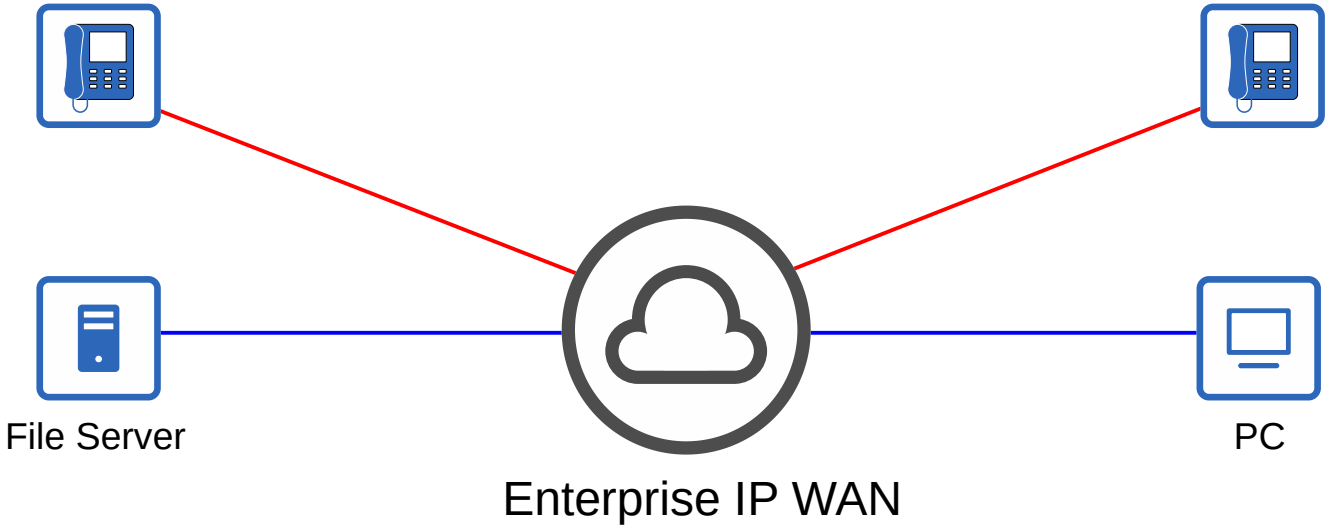
- Voice traffic and data traffic used to use entirely separate networks.
  → Voice traffic used the PSTN
  → Data traffic used the IP network (enterprise WAN, Internet, etc)

- QoS wasn't necessary as the different kinds of traffic didn't compete for bandwidth.



Quality of Service (QoS)

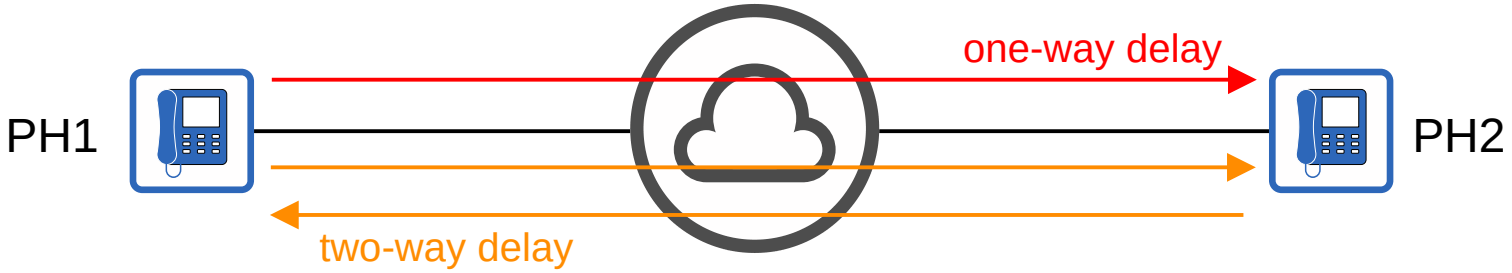
- Modern networks are typically *converged networks* in which IP phones, video traffic, regular data traffic, etc all share the same IP network.
- This enable cost savings as well as more advanced features for voice and video traffic, for example integrations with collaboration software (Cisco WebEx, Microsoft Teams, etc).
- However, the different kinds of traffic now have to compete for bandwidth.
- QoS is a set of tools used by network devices to apply different treatment to different packets.



Quality of Service (QoS)

- QoS is used to manage the following characteristics of network traffic:
  1) **Bandwidth**
  → The overall capacity of the link, measured in bits per second (Kbps, Mbps, Gbps, etc)
  → QoS tools allow you to reserve a certain amount of a link's bandwidth for specific kinds of traffic.
  For example: 20% voice traffic, 30% for specific kinds of data traffic, leaving 50% for all other traffic.

  2) **Delay**
  → The amount of time it takes traffic to go from source to destination = **one-way delay**
  → The amount of time it takes traffic to go from source to destination and return = **two-way delay**



Quality of Service (QoS)

- QoS is used to manage the following characteristics of network traffic:

  1) **Bandwidth**
  → The overall capacity of the link, measured in bits per second (Kbps, Mbps, Gbps, etc)
  → QoS tools allow you to reserve a certain amount of a link's bandwidth for specific kinds of traffic.
  For example: 20% voice traffic, 30% for specific kinds of data traffic, leaving 50% for all other traffic.

  2) **Delay**
  → The amount of time it takes traffic to go from source to destination = **one-way delay**
  → The amount of time it takes traffic to go from source to destination and return = **two-way delay**

  3) **Jitter**
  → The variation in one-way delay between packets sent by the same application
  → IP phones have a 'jitter buffer' to provide a fixed delay to audio packets.

  4) **Loss**
  → The % of packets sent that do not reach their destination
  → Can be caused by faulty cables.
  → Can also be caused when a device's packet *queues* get full and the device starts discarding packets.

Quality of Service (QoS)

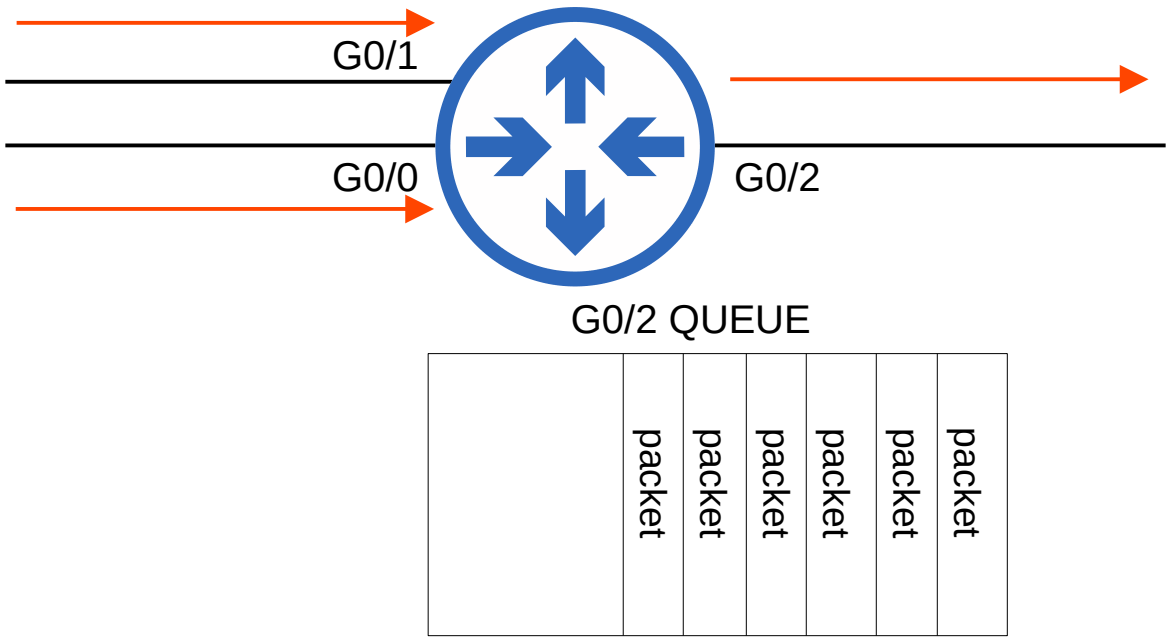
- The following standards are recommended for acceptable interactive audio (ie. phone call) quality:

  One-way delay: 150 ms or less
  Jitter: 30 ms or less
  Loss: 1% or less

- If these standards are not met, there could be a noticeable reduction in the quality of the phone call.

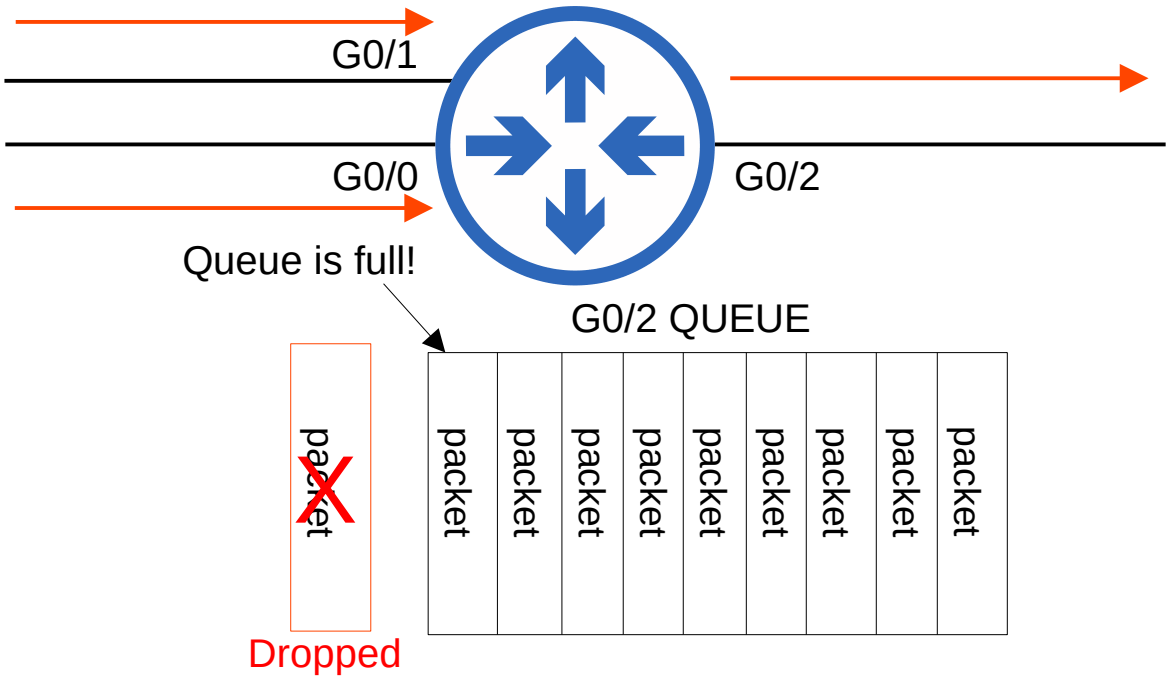
QoS - Queuing

- If a network device receives messages faster than it can forward them out of the appropriate interface, the messages are placed in a queue.
- By default, queued messages will be forwarded in a First In First Out (FIFO) manner.
  → Messages will be sent in the order they are received.



QoS - Queuing

- If a network device receives messages faster than it can forward them out of the appropriate interface, the messages are placed in a queue.
- By default, queued messages will be forwarded in a First In First Out (FIFO) manner.
  → Messages will be sent in the order they are received.
- If the queue is full new packets will be dropped.
- This is called *tail drop*.



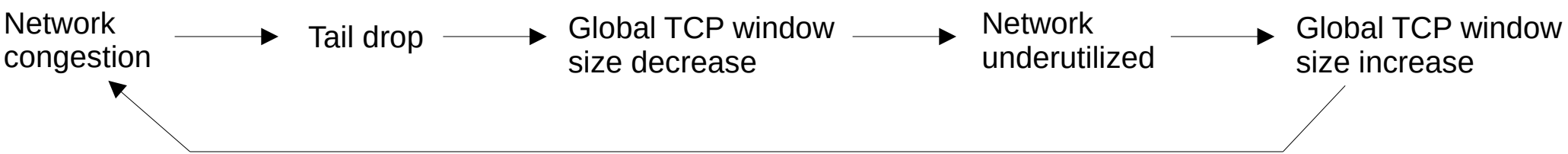
QoS – Queuing

- **Tail drop** is harmful because it can lead to **TCP global synchronization**.

- Review of the **TCP sliding window**:
  → Hosts using TCP use the 'sliding window' increase/decrease the rate at which they send traffic as needed.
  → When a packet is dropped it will be re-transmitted.
  → When a drop occurs, the sender will reduce the rate it sends traffic.
  → It will then gradually increase the rate again.

- When the queue fills up and **tail drop** occurs, all TCP hosts sending traffic will slow down the rate at which they send traffic.

- They will all then increase the rate at which they send traffic, which rapidly leads to more congestion, dropped packets, and the process repeats again.



QoS - Queuing

- A solution to prevent tail drop and TCP global synchronization is **Random Early Detection** (RED).
- When the amount of traffic in the queue reaches a certain threshold, the device will start randomly dropping packets from select TCP flows.
- Those TCP flows that dropped packets will reduce the rate at which traffic is sent, but you will avoid global TCP synchronization, in which ALL TCP flows reduce and then increase the rate of transmission at the same time in waves.
- In standard RED, all kinds of traffic are treated the same.
- An improved version, **Weighted Random Early Detection** (WRED), allows you to control which packets are dropped depending on the traffic class.
- We will cover traffic classes and details about how QoS actually works in the next video.

Things we covered

- IP Phones/Voice VLANs
- Power over Ethernet (PoE)
- Intro to Quality of Service (QoS)

Quiz 1

Examine G0/0's interface configuration. Which of the following statements are true? (select two)

```
SW1(config)#interface gigabitethernet0/0
SW1(config-if)#switchport mode access
SW1(config-if)#switchport voice vlan 99
```

a) Voice traffic received by G0/0 should be tagged in VLAN 99.

b) Voice traffic received by G0/0 should be untagged.

c) Data traffic received by G0/0 should be tagged in VLAN 1.

d) Data traffic received by G0/0 should be untagged.

e) Data traffic received by G0/0 should be discarded.

f) G0/0 will operate as a trunk.

Quiz 2

You issue the **`power inline police`** command on a PoE-enabled switch port. What will happen if the connected device draws too much power from the switch?

a) A Syslog message will be generated.

b) The interface will be restarted and a Syslog message will be generated.

c) The interface will be err-disabled and a Syslog message will be generated.

d) The interface will be shutdown.

Quiz 3

Which of the following are recommended standards for acceptable interactive audio quality? (select three)

a) Delay: 30 ms or less

b) Delay: 150 ms or less

c) Jitter: 30 ms or less

d) Jitter: 50 ms or less

e) Loss: 1% or less

f) Loss: 2% or less

Quiz 4

Which of the following is a negative effect of tail drop?

a) TCP sliding window

b) RED

c) WRED

d) TCP global synchronization

Quiz 5

Which of the following is the default manner of forwarding queued packets?

a) FIFO

b) CBWFQ

c) RED

d) WRED