PHONES

Ports on the back of a phone

- RS-232—Expansion modules like 7914, 7915, 7916
- 10/100 SW—To the network
- 10/100 PC—To a computer, printer, etc.

PoE (Power over Ethernet) can be Cisco pre-standard or 802.3af, or the phone can use a 48 VDC power brick. PoE eliminates cord clutter and allows a central UPS. Adding a sidecar to the phone (more line buttons) may outstrip the capabilities of PoE. 802.3at increases PoE from 15.4 watts (802.3af) to 25.5 watts.

Many Cisco switches provide PoE. If they don't it can be added to Ethernet using an injector for one line or a power patch panel for many lines.

VLANS

VLAN = Broadcast Domain = IP Subnet. VLANs provide increased performance, improved manageability, physical topology independence (users in the same VLAN can be spread across the network), and increased security. Trunk ("tagged") ports carry VLANs between switches. Trunk headers are added & removed as the frame enters / leaves the trunk; the host never sees them. Separate voice VLANs prevent packet sniffing PCs from capturing the audio. They also make QoS (Quality of Service) prioritization easier. Some NICs (Network Interface Cards) can read VLAN tags, allowing a server to serve many VLANs at once through a trunk connection to the switch.

802.1Q is the standard for VLAN tagging.

Voice VLANs—Voice packets are tagged, data packets from the attached PC are untagged. This arrangement is called a multi-vlan access port and is more secure than a true trunk to the phone, which would enable a hacker to attach a switch.

```
S1(config)# vlan 10
S1(config-vlan)# name VOICE
S1(config-vlan)# vlan 50
S1(config-vlan)# name DATA

S1(config-if)# switchport mode access
S1(config-if)# spanning-tree portfast
                    This handles the fact that phones boot quickly and make DHCP requests before STP is ready.
S1(config-if)# switchport access vlan 50
S1(config-if)# switchport voice vlan 10
                    NOTE: setting a voice VLAN automatically enables portfast, so above unnecessary
S1# switchport show vlan brief
S1# switchport show interfaces fa0/1 switchport
                    Show voice vlan on a swithcport; there are no shortcuts like for data vlans (show interf status)
```

Cisco phones learn which VLAN to use from CDP. Non-Cisco phones need to be configured.

PHONE BOOT & CONFIGURATION

Overview

- Phone powers on, perhaps using PoE
- Switch uses CDP (Cisco Discovery Protocol) to tell phone which VLAN to use for voice
- Phone sends DHCP request (broadcast within the voice VLAN
- When phone accepts DHCP offer, it gets DNS server address, domain name, gateway, and option 150—the address of a TFTP server for telephone configs
- Phone downloads its configuration and firmware from the option 150 TFTP server. That config file contains a list of call processing (CUCM or CME) agents
- Starting with the first processing agent (aka server) in the list (the primary), the phone attempts to contact the agent to register via SCCP or SIP. There can be up to 3 agents in the list. If it can't register with any of them, it reboots. Most Cisco phones use the proprietary SCCP; SIP is vendor-neutral. The phone identifies itself by its MAC address.
- The call processing server performs a lookup and sends the operating config to the phone

Configuration Files—A phone configured in CUCM or CME will have a config file on the server called SEP< *MAC*>*.cnf.xml,* where MAC is the MAC address of the phone and SEP happens to stand for "Selsius Ethernet Phone." Selsius was acquired by Cisco. If no file exists for a phone's MAC address, the phone will try to download XMLDefault.cnf.xml, a base config file used for auto-registration, where phones can register themselves without being configured. The config file contains the IP address and port number for the call processing server (CME/CUCM). Actually, it contains up to three, for redundancy.

Registration & Signaling Protocols—The phone registers with the server mentioned in its configuration file using one of two protocols. Various phone models support one or both. Following registration, the chosen protocol continues to be the method of communication between the phone and its server; the server uses it to send a detailed operating config to the phone and the phone uses it to place calls.

- SCCP (Skinny Client Control Protocol)—A Ciscoism begin phased out
- SIP (Session Initiation Protocol)—Vendor-neutral, evolving to become a more capable industry standard.

Configuration Sources (recap)

	SUPPLIER	METHOD	CONTENTS
Configuration File (.xml)	TFTP Server	TFTP	Device language, firmware revision, call processing server IP addresses, port numbers, etc.
Operating Configuration	Call Processing Server (CUCM or CME)	SCCP or SIP	directory/line numbers, ring tones, softkey layout (on-screen buttons)

DHCP

This example creates runs a server in two subnets (scopes), our data VLAN and our voice VLAN.

```
R1(config)# ip dhcp excluded-address 172.16.1.1 172.16.1.9
R1(config)# ip dhcp excluded-address 172.16.2.1 172.16.2.9
```
Type exclusions first, before the (running) router has a chance to give out those addresses
The two addresses on each line represent a beginning and end of the excluded range
```
R1(config)# ip dhcp pool DATA_SCOPE
R1(dhcp-config)# network 172.16.2.0 255.255.255.0
R1(dhcp-config)# default-router 172.16.2.1
R1(dhcp-config)# dns-server 4.2.2.2 [ 4.3.3.3 … ]
R1(dhcp-config)# ip dhcp pool VOICE_SCOPE
R1(dhcp-config)# network 172.16.1.0 255.255.255.0
R1(dhcp-config)# default-router 172.16.1.1
R1(dhcp-config)# option 150 ip 172.16.1.1
```
The TFTP server holding config file for the phone
```
R1# show ip dhcp binding
```
See which DHCP addresses are in use and by what MAC address

If you've centralized DHCP service somewhere else, you may need to use

```
R1(config-if)# ip helper-address 10.0.0.12
```
Tells the address of a central DHCP server. Note this is per-interface & therefore per (sub)net.

NTP

Cisco devices show March 1, 1993 when they boot up without having their clock set.

```
R1(config)# ntp server 64.209.210.20
```
Multiple sources add redundancy but only one is used at a time
```
R1(config)# clock timezone PST -8
```
PST appears to be solely for human readability; the -8 is what matters
```
R1(config)# clock summer-time PDT recurring
```
Recurring tells it to use the normal rules for begin/end instead of you typing them
```
R1# show ntp associations
R1# show clock
```

You can also have the router act as an NTP server and pass the time on to others

```
R1(config)# ntp master 4
```
4 is the stratum number (a radio clock is 1). Just add 1 to the "st" column in the associations cmd

QUALITY OF SERVICE

QoS—"the ability of the network to provide better or special service to a set of users and applications at the expense of other users and applications" [the Cisco definition per book]. When applied, Cisco QoS always marks packets for preference but nothing actually happens until an interface is congested and winners must be chosen.

Traffic Characteristics—data traffic can vary wildly, at the mercy of individual transfers. Voice has a consistent load with lots of tiny packets. Video is more variable, based on the amount of movement in an image, thanks to compression.

Voice & Video Requirements—In addition to sufficient bandwidth

- Delay—150ms or less, end-to-end. Can be fixed or variable (can be changed by moving voice packets forward in queue)
- Jitter (delay variation)—30ms or less (This is 1.5 default samples; packetization = 20ms)
- Packet loss—1% or less

Types of Data Traffic

- Mission-Critical—need dedicated bandwidth amounts
- Transactional—Interactive, requiring rapid response
- Best-Effort—Web, FTP, etc.
- Scavenger—No business need, but lots of bandwidth. Bittorrent, etc.

QoS Mechanisms

- Best Effort—Default. No QoS in use
- IntServ (Integrated Services)—Reserved bandwidth, end-to-end. Scalability & waste problems
- DiffServ—Traffic classes (almost guaranteed bandwidth). Most often used

Tool Categories

- Classification & Marking—Layer 2 or 3 marking (routers can only read the L_3 marks)
- Congestion Management—Once a link is saturated, which queued packet goes first
- Congestion Avoidance—Preventatively drop less-essential packets
- Policing & Shaping—Limit the bandwidth of hogs. Designed for links for a lower speed than physical speed. Shaping queues for later sending (smoothing), policing drops.
- Link Efficiency—on low speed links
  - Serialization Delay—time to feed a packet onto the link—longer on slower links, like a slow turnstile. Compressing data might actually improve latency.

    Math Example: Serialization Delay for a 1500-byte packet on a 56 kbps link
    = 1500 * 8 / 56000 = 214ms

Link Efficiency Mechanisms—Cisco doesn't recommend for links ≥ T1 (1.544 Mbps)

- Payload Compression
- Header Compression—RTP audio has lots of small packets
  - cRTP (compressed Real-time Transport Protocol)—Reduces a 40-byte header to 2-4
- LFI (Link Fragmentation and Interleaving)—Chops up large (non-voice) packets to interleave voice. Available when using Multilink PPP or one of two Frame Relay options

Queuing Algorithms—used when congestion occurs (FIFO is default for most interface types)

- WFQ (Weighted Fair Queuing)—Balance between senders; discriminate against chattiness
- CBWFQ (Class-Based Weighted Fair Queuing)—Guarantee bandwidth % to various classes of traffic, rest is WFQ
- LLQ (Low Latency Queuing)—Preferred voice solution. AKA PQ-CBWFQ because it adds a priority queu e to CBWFQ. Traffic in the priority queue gets first bandwidth, not just a guaranteed amount. Used by Cisco's AutoQoS, discussed next.

Router QoS Possibilities

QoS method	entering Router	Exiting Router
Classification	•	
Marking	•	•
Congestion Management		•
Congestion Avoidance		•
Shaping		•
Policing	•	•
Compression		•
Fragmentation & Interleaving		•

Cisco AutoQoS—One command turns on/off at interface; many commands show up in running config as result, implementing Cisco best practices for the bandwidth & encapsulation on that interface. Advantages over manual configuration:

- Speed of deployment
- Consistency of Configuration
- Reduced expertise cost
- Allows manual tuning

Trust Boundary—where in the network you believe QoS category markings aren't being spoofed. Cisco IP Phones can mark their own traffic and be trusted because CDP will notice if the phone is replaced with another device. Some switches can mark traffic at the access layer, otherwise the distribution layer must handle it. This is usually OK because the access layer rarely has bottlenecks

Configuring AutoQos—Ensure correct bandwidth entered on serial lines first; routers can't audo-detect serial speed (!) [Valentine p. 76, Ciaora p. 160]. Command varies with location:

- access port

```
S(config-if)# auto qos voip { cisco-phone | cisco-softphone }
```

With cisco-phone and softphone, CDP controls the trust boundary, detecting ACTUAL presence

- switch uplink to router

```
S(config-if)# auto qos voip trust
```

You consider traffic markings coming from the router to be trustworthy

- router interface

```
R(config-if)# auto qos voip trust
```

Many of the changes (phantom commands) are not under the interface, itself

```
R(config-if)# auto discovery
```

Alternative version of AutoQoS that monitors traffic over time and recommends QoS policies

Commands used to configure AutoQoS

Command	Router /Switch	Description (p.166 table 6-8)
`auto qos voip`	R	Enable QoS. Don't trust existing marks, remark using access lists or NBAR (below)
`auto qos voip trust`	R or S	Enable QoS. Trust markings.
`auto qos voip cisco-phone`	R or S	Enable QoS. Trust markings only if CDP detects a Cisco IP phone
`auto qos voip cisco-softphone`	R or S	Enable QoS. Trust markings only if CDP detects a Cisco IP softphone (e.g. Cisco IP Communicator)

NBAR (Network-Based Application Recognition)—Automated marking based on content at the cost of processor load.

COS(Class of Service)—QoS markings in L2 packet header

TOS(Type of Service)—QoS markings in L3 packet header