Organizational Documents

DOMAIN 3.0

MODULE 13

Organizational Documents Topics

Plans and Procedures

Security Policies

Loss Prevention

Common Agreements

Common Documentation

Structured Cabling - MDF and IDF

Horizontal and Vertical Cabling

Labeling

Surveys and Assessments

Plans and Procedures

On-boarding and Off-boarding Procedures

On-boarding and off-boarding an employee are not single events, but a series of tasks designed to make the transition as smooth as possible

Both on-boarding and off-boarding will include checklists and steps for management, the employee, HR, and the IT department

Since most work processes involve IT, it is crucial that both on-boarding and off-boarding maintain the integrity and security of the network, its resources, and processes

IT On-boarding Tasks

The IT team must coordinate with the department that hires the new employee

Ensure that:

- The employee’s workstation is ready
- The login account is ready for use with a temporary password
  - Assigned to the correct groups and given required permissions
- Any additional authentication mechanisms are ready (RFID cards, badges, RSA tokens, etc.)
- Assigned hardware is provisioned, cleaned, and ready to be issued

The IT team should also do their part in making the new hire feel welcome

- Give them a point of contact for IT-related questions and issues

Depending on the environment, be prepared to enforce/revoke network privileges if the user fails to complete required security training in the allotted time

IT Off-boarding Tasks

HR and management will conduct their own offboarding tasks, including necessary paperwork an exit interview

The IT department must assist with employee offboarding by:

- Collecting, validating, and signing off on returned equipment
- Suspending the user’s account and revoking privileges
- Ensuring that the user no longer has access to the network, systems, or facilities
- Coordinate with the security team, especially if the termination is involuntary or unfriendly

Change Management

Attempts to ensures that all changes to your IT infrastructure are assessed, approved, implemented and reviewed in a controlled way

Steps to IT infrastructure change:

1. Formally requesting a change
2. Reviewing any requested changes
3. Approving any requested changes
4. Creating a detailed project plan for changes
5. Reviewing and refining the plan. This is done by a team of stakeholders.
6. Planning or scheduling the implementation of changes
7. Testing the change
8. Assessing and reporting on the results of the change

Change Management Documentation

Used to establish the process for managing change within a network

Documents how changes will be proposed, accepted, monitored, and controlled

Includes instructions for each type of change

Specifies versioning format for tagging documents under its control

Business Continuity Plan (BCP)

A document that outlines how a business will continue operating during an unplanned disruption in service

Contains contingencies for business processes, assets, human resources and business partners

- Every aspect of the business that might be affected

Typically contain a checklist that includes:

- supplies and equipment
- data backups
- backup site locations

Identifies plan administrators

Includes contact information for emergency responders, key personnel and backup site providers

May provide detailed strategies on how business operations can be maintained for both short-term and long-term outages

Disaster Recovery Plan

Part of the BCP

Focused on IT infrastructure and services

Contains detailed instructions on how to respond to--and minimize the effects of--major disruptions:

- Natural disasters
- Loss of access to a location
- Loss of systems or data
- Power outages
- Communications outages
- Terrorism
- Cyber attacks
- Any other disruptive event

Outlines the order in which services and functions will be restored

- Includes the RTO and RPO of each service type

Incident Response Plan

A set of established procedures to address the consequences of a specific IT event

- Typically security related
- Smaller than a disaster

Quickly and effectively detect, manage and recover from an attack

- Try to minimize damage to business assets

Usually contains information regarding:

- Who is in the incident response team
- Team member roles and responsibilities
- Technological tools
- Communications during the incident
- Steps to take to minimize damage
- Evidence collection and handling
- Post mortem analysis and steps to reduce future risk

Standard Operating Procedure (SoP)

Best practice for executing tasks

Hardware and software planning and maintenance

Incident and change management

The top layer of documents that are shared with customer

Usually do not contain confidential information

Procedures Document

More detailed than SOP

Usually product-specific but implementation-generic

Sometimes contain description of the steps and visuals

May include use cases and workflow diagrams

Documents will be use during audits

Work Instructions

Instructions to perform a specific piece of work

Specific to your environment

May just be a series of bullet points or high-level steps

- Will then depend on procedure documents for exact steps

Baseline Configurations

A baseline is the minimum required configuration for a system

It is the starting configuration for a newly provisioned device

- It ensures that all devices provide a minimum level of features, functionality, and performance

The baseline is also the target for a device that must be refreshed / wiped clean

Baselines typically include:

- Required software
- Network settings
- Security settings
- Patch levels
- Hardware levels

An organization will have a company-wide baseline

Individual departments may have additional baseline requirements on top of the company minimum

Security Policies

What is an IT Security Policy?

Identifies the rules and for all individuals accessing and using an organization's IT assets and resources

Typically a collection of smaller policies that each address a particular aspect of security

- Acceptable Use Policy
- Backup Policy
- Incident Response Policy
- Virtual Private Network (VPN) Policy
- Wireless Policy
- Network Security Policy
- Confidential Data Policy
- Mobile Device Policy
- Outsourcing Policy
- E-mail Policy
- Password Policy
- Network Access Policy
- Remote Access Policy
- Guest Access Policy
- Third Party Connection Policy
- Encryption Policy
- Data Classification Policy
- Retention Policy
- Physical Security Policy

Security Policy Benefits

Helps the organization to:

- Comply with international, federal, state, and local regulations
- Adhere to best practices
- Fulfill audit requirements
- Reduce legal risk
- Mitigate risk from a security incident
- Satisfy partners, customers, etc.
- Educate users on sound security practices

Any policy must be accompanied by good training and enforcement

Keep in mind that the *best* way to enforce any policy is to put technical controls in place

- The user will automatically have to comply without you constantly policing them

Bring Your Own Device (BYOD) Policy

Employees bring and use their own mobile devices at work

BYOD saves the organization money and is convenient for users
- Users can have the phone they are comfortable with
- They don’t need to carry two phones

BYOD also introduces security risks and can be a headache for the IT dept.
- Many types of devices
- Question of phone number ownership

The BYOD policy should include:
- Acceptable use during business hours
- On-site functionality restrictions (i.e. no recording in certain areas)
- Agreement to place device under mobile device management (MDM) control
- Support/repair/replacement limits
- Separation of personal and business data
- Understanding that the company can track all activity/data on a BYOD phone
- Understanding that, In case of law enforcement/legal action, the phone might be confiscated for a long time

The company may prefer Select/Choose Your Own Device

Acceptable Use Policy (AUP)

A set of rules that specifies practices and restrictions a user agrees to for access to an organization’s network/Internet

For example, do not use the network or system to:

- Share credentials or use another’s credentials on the network
- Harass others
- Violate the law, regulations, or company rules
- Conduct other commercial business
- Make illegal copies of copyrighted materials including software
- Gain access to restricted systems
- Store confidential/classified information on removable media

The AUP should make it clear to employees that they can have no expectation of privacy when using company equipment

It should also include consequences for infractions and violations

Password Policy

States password requirements including:

- Password length
- Complexity
- Expiration
- History
- Confidentiality of credentials

Privileged User Agreement

For users who require escalated access to network devices or confidential/classified data

Typically the user is only allowed to use the privileged account for the required task

- For normal activities, the user must use a separate unprivileged account

An organization might require special credentials for privileged access

- Two-factor authentication
- Longer password
- Restricted hours/locations

Auditing users when logged on with escalated privileges is recommended

You should regularly review who has privileged accounts

- If possible, use automated policy mechanisms to return privileged group membership to baseline

Remote Access Policy

Remote access adds security risk

A remote access policy can include:

- Hardware and software configuration standards for remote access, including anti-malware, firewalls, and antivirus
- Encryption requirements
- Information security, confidentiality, and email policies
- Physical and virtual device security
- Access privileges
- Connectivity guidelines
- Authentication requirements
- Acceptable use
- Third-party protections and standards (trusted vs. non-trusted sources or hosts)
- Policy compliance, governance, and enforcement
- Access and equipment ownership requirements

Safety Procedures and Policies

An organization should always have written safety policies and procedures

Everyone should be trained in these policies and procedures

Policy is the overarching statement of what management wants

Procedures are the actual steps/tasks taken to fulfill policy

Licensing Restrictions

Detect and disallow unlicensed software

Ensure that software, including evaluation copies, is used according to its EULA

Determine which devices and users are authorized for software installation/use

Identify which group will pay for the license
- IT dept
- Line of business
- Parent company

Keep track of subscription renewals
- Be able to transfer licenses from one user to another

Ensure the correct installer is available for the license type
- Different license types may have their own installers for the same product

Test updated versions before release into production

International Export Controls

U.S. export regulations control whether certain commodities, software and information can be transmitted outside the U.S.

IT department must help the organization stay in compliance

- Physical shipment
- File transfers
- Encryption levels
- Sensitive data such as classified information, SBU Noforn, PII and PHI

Legal department needs to advise you

You can employ third-party verification of compliance

Loss Prevention

Inventory Management

The process of keeping records of network assets

Enables network administrators/businesses to have a physical record of network equipment within the organization

- Improves efficiency
- Reduces cost
- Facilitates reports and analytics
- Allows managers to keep track of assets and plan their purchasing/replacement cycles

Organization has knowledge of ROI, size of network

Assigns responsibility to departments / teams

- Regular inventory updates help deter theft

May include:

- Number of devices, vendor, serial numbers, installation information
- IP addresses of all devices, IP addressing segments used
- Software types, names, license keys and expiration dates
- Last inventory scanning date
- Last known location / owner of asset

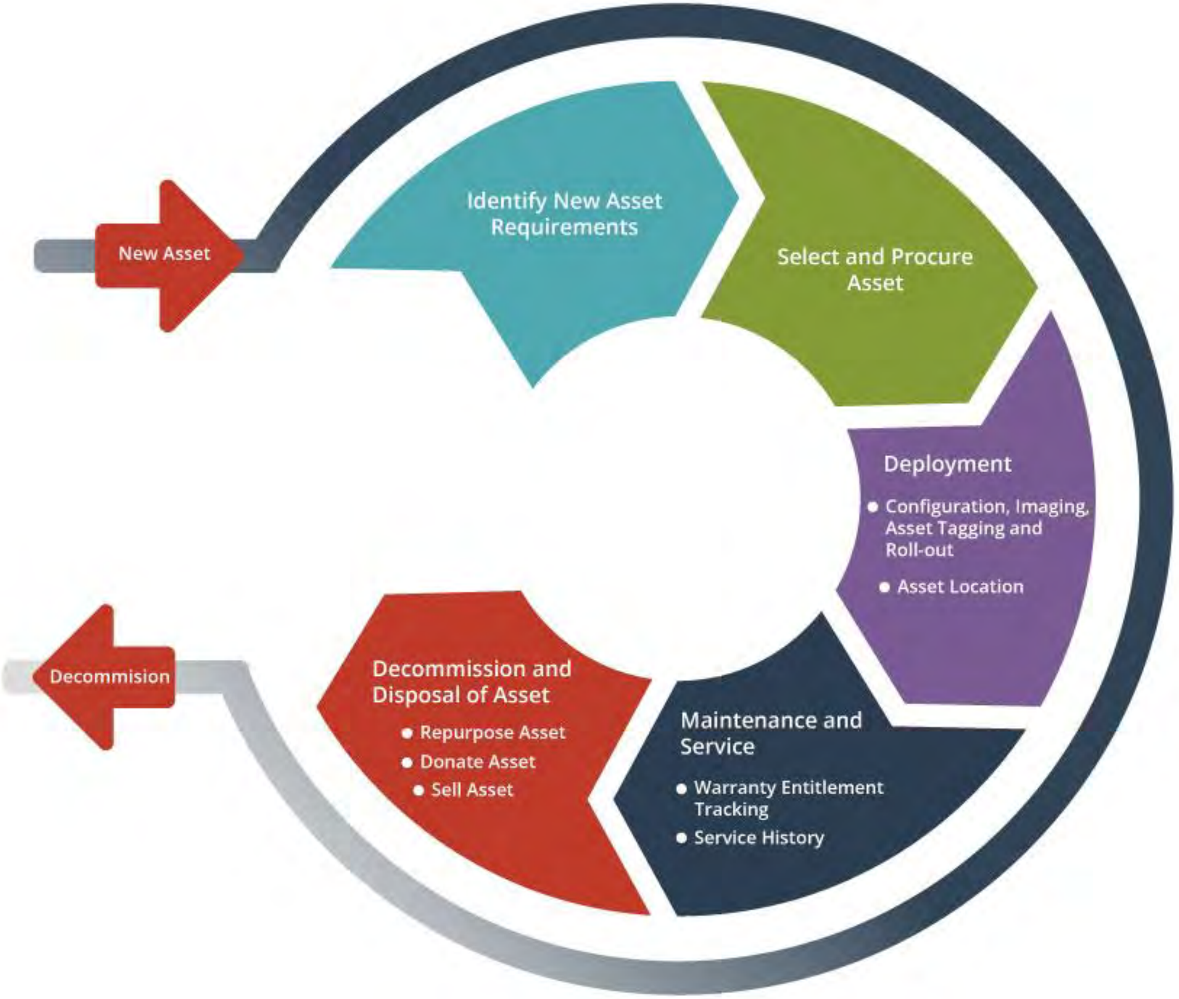
System Life Cycle

A visualization of the entire life of an IT asset including:

- Needs assessment
- Procurement
- Deployment
- Maintenance
- Decommissioning / Disposal

Each phase of the system's life has its own management and security considerations

You should have system life cycle documentation to standardize how you identify, purchase, deploy, maintain, and decommission/dispose of assets



Asset Disposal

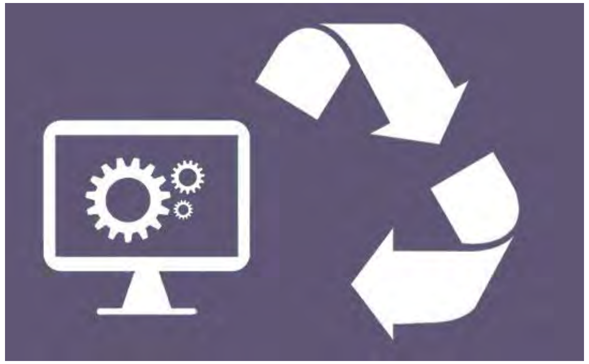
Part of your system lifecycle documentation

IT assets require not only ethical disposal of equipment but also the complete destruction and inability for organization’s data to be accessed

- Recycling

Ensure erasure and data destruction to eliminate risks of data breach the equipment disposition

Networking devices, routers, and switches hold sensitive information that could be used to find entry to or otherwise compromise an organization’s network



Data Loss Prevention

The attempt to minimize/prevent data loss or leakage (exfiltration)

Can include:

- Policies and procedures (including for print jobs and removable media)
- Firewalls
- DLP applications and services
- Client policies
- IDS/IPS
- Digital rights management (DRM)
- Physical controls

You should have a DLP document explaining what data you are trying to protect, the risks to that data, and what you are doing to mitigate those risks

Common Causes of Data Loss/Leakage

Malicious or careless employees

“Reply All” email

Unprotected print jobs

Removable media

Laptops and mobile devices

Copy/paste activities

Insufficiently protected physical environment

Social media, instant messaging

Cell phone cameras

Social engineering

Trash/recycled paper

Network applications

File upload/sharing activities

Viruses/hacking

Insufficient segregation of sensitive network segments

Equipment or asset theft

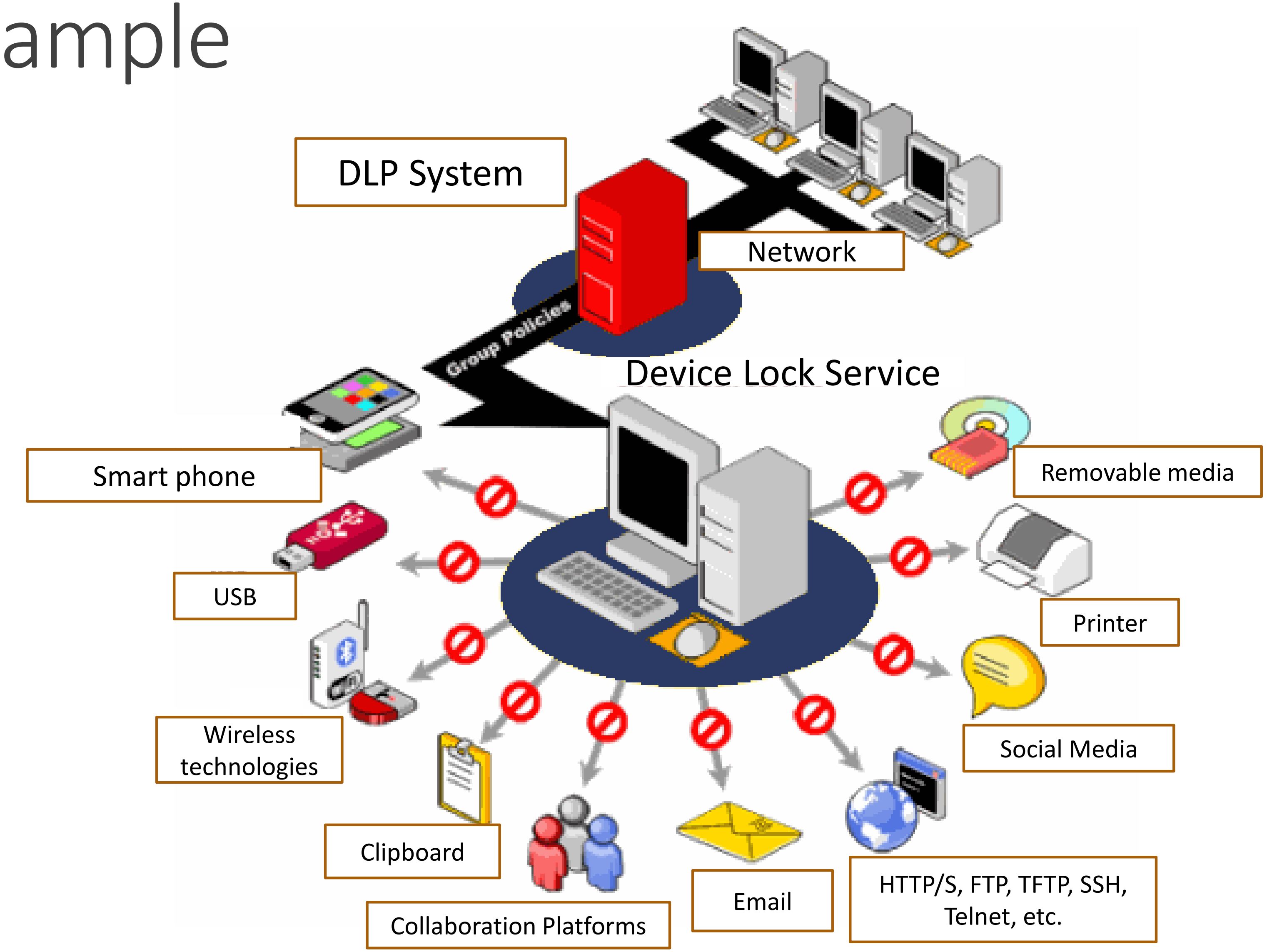
Improperly configured devices

Vulnerable network

Vulnerable servers, websites, and applications

Public-facing computer monitors

DLP Example


DLP System
Network
Group Policies
Device Lock Service
Smart phone
USB
Wireless technologies
Clipboard
Collaboration Platforms
Email
HTTP/S, FTP, TFTP, SSH, Telnet, etc.
Social Media
Printer
Removable media

Common Agreements

Non-Disclosure Agreement (NDA)

Also known as a confidentiality agreement

A legally binding contract

One party agrees to give a second party confidential information business/products

Second party agrees not to share this information with anyone else for a period of time

Used to protect sensitive information and intellectual property

Outlines in detail what information remains private and what information can be shared

Service Level Agreement (SLA)

A Service Level Agreement is a contracted commitment by a provider

Formally defines "what you get" in terms of uptime/availability

MTBF and MTTR figure prominently in the guarantees of an SLA

Clearly states metrics, responsibilities and expectations from both the vendor and customer in the event of issues

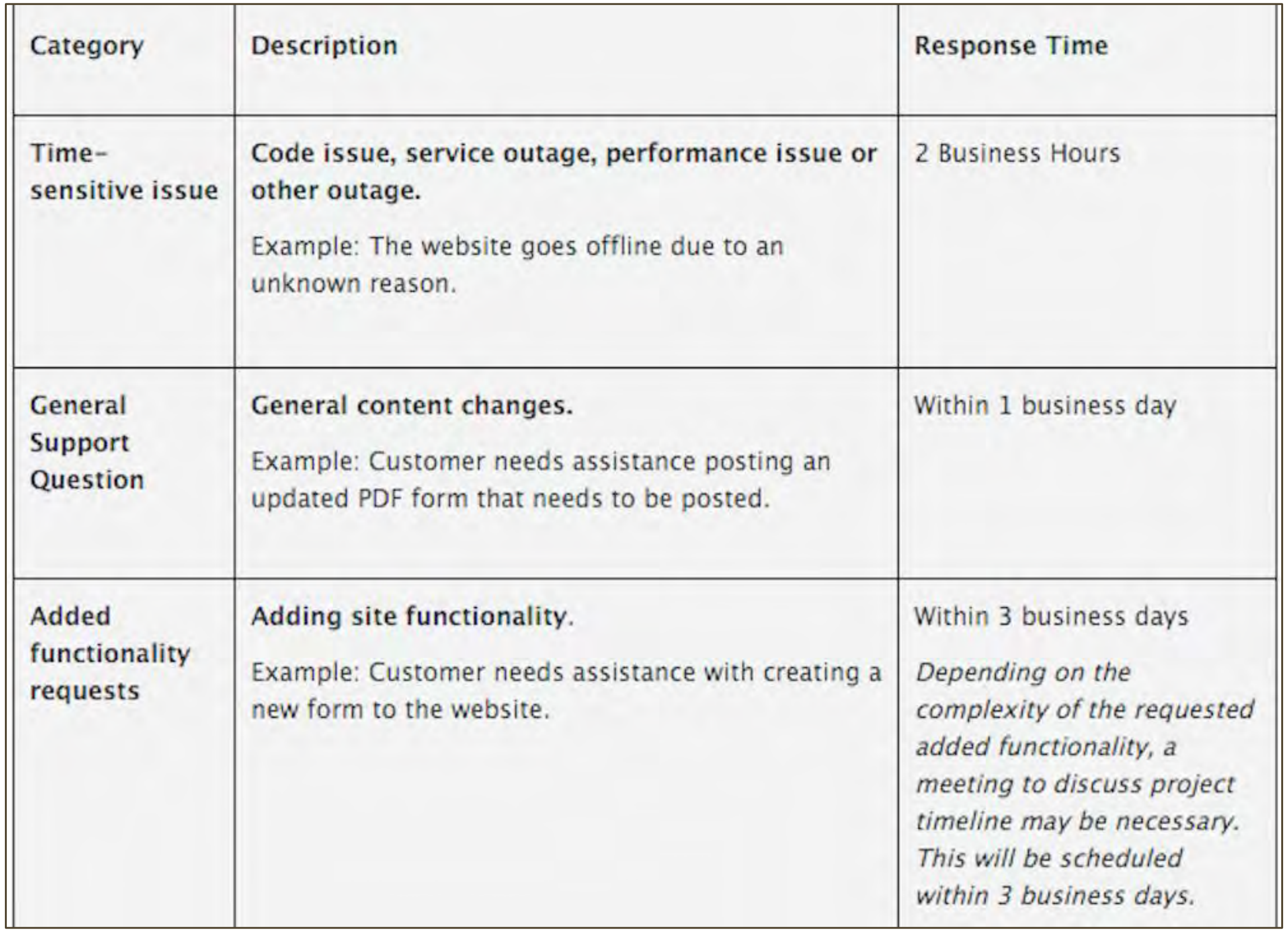
Ensures both vendor and organization have the same understanding of requirements

- Specifies how many incidents and of what type fall under the SLA
- Typically offers the customer the ability to pay for additional premium service, outside of the SLA

Should specify who is authorized on the client side to:

- Contact the vendor in case of an issue
- Determine the level of support requested

SLA Example



Category	Description	Response Time
Time-sensitive issue	**Code issue, service outage, performance issue or other outage.** Example: The website goes offline due to an unknown reason.	2 Business Hours
General Support Question	**General content changes.** Example: Customer needs assistance posting an updated PDF form that needs to be posted.	Within 1 business day
Added functionality requests	**Adding site functionality.** Example: Customer needs assistance with creating a new form to the website.	Within 3 business days *Depending on the complexity of the requested added functionality, a meeting to discuss project timeline may be necessary. This will be scheduled within 3 business days.*

Memorandum of Understanding (MOU)

An agreement between two or more parties outlined in a formal document

Not legally binding

- Signals the willingness of the parties to move forward with a contract

Describes the broad outlines of an agreement that two or more parties have reached

- Clearly outlines specific points of understanding
- Names the parties
- Describes the project on which they are agreeing, including scope, and details each party's roles and responsibilities

AKA Letter of Intent (US)

Common Documentation

Diagram Symbols

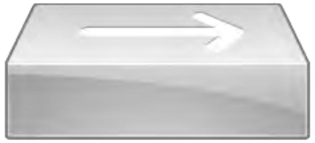
A network diagram is a visual representation of an actual system

Diagrams rely on symbols (icons) to convey meaning

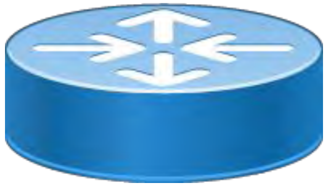
The symbols should be recognizable and consistent

Important for planning, implementation, and change management

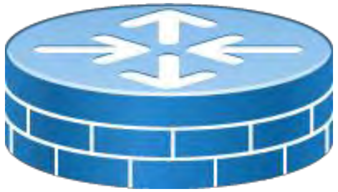
Common Cisco Icons



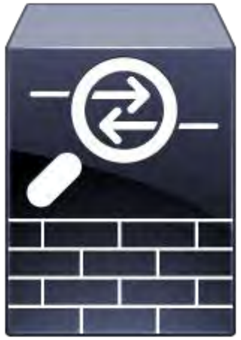
Hub



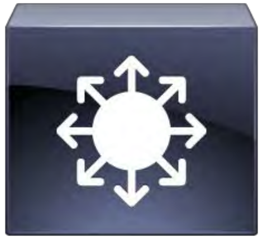
Router



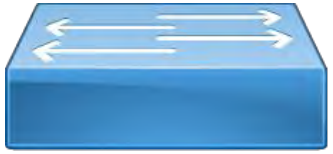
Router w Firewall



ASA

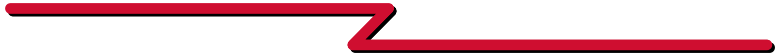


Multilayer Switch

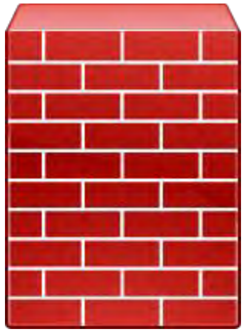


Switch

Ethernet Link

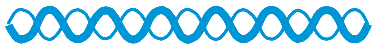


Serial Link

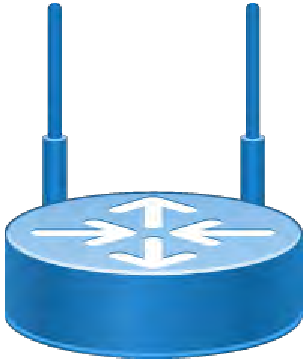


Firewall

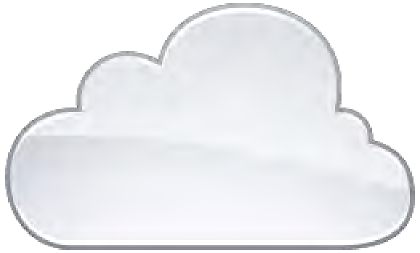
Common Cisco Icons (cont'd)



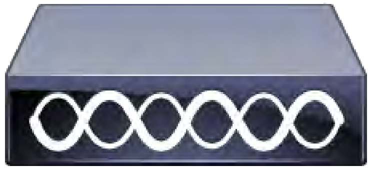
Wireless Link



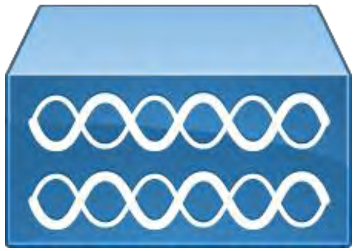
Wireless Router



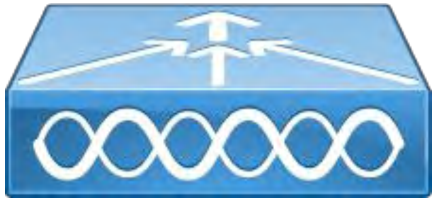
WAN Cloud



Wireless Access Point

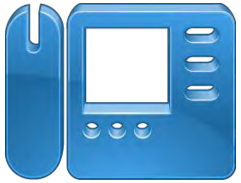


Dual Band Wireless Access Point

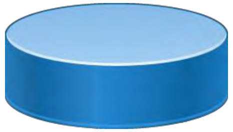


Wireless Controller

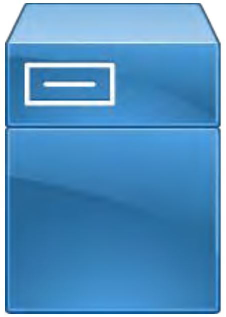
Common Cisco Icons (cont'd)



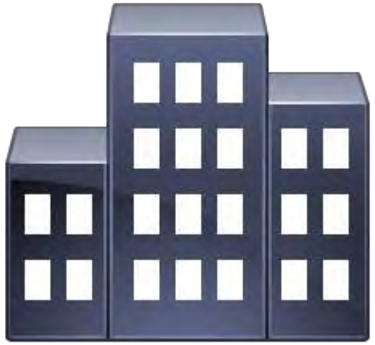
Phone



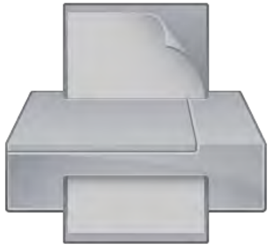
Database



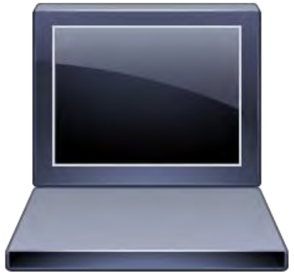
Server



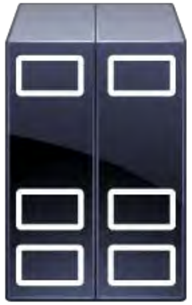
Generic Building



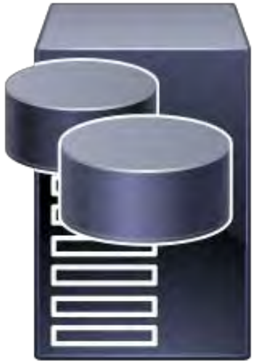
Printer



Laptop



Standard Host



Storage Array

Logical Network Diagram

AKA Logical Topology

Used by technicians to trace/troubleshoot the flow of data

Focused more on electrical connectivity than physical location

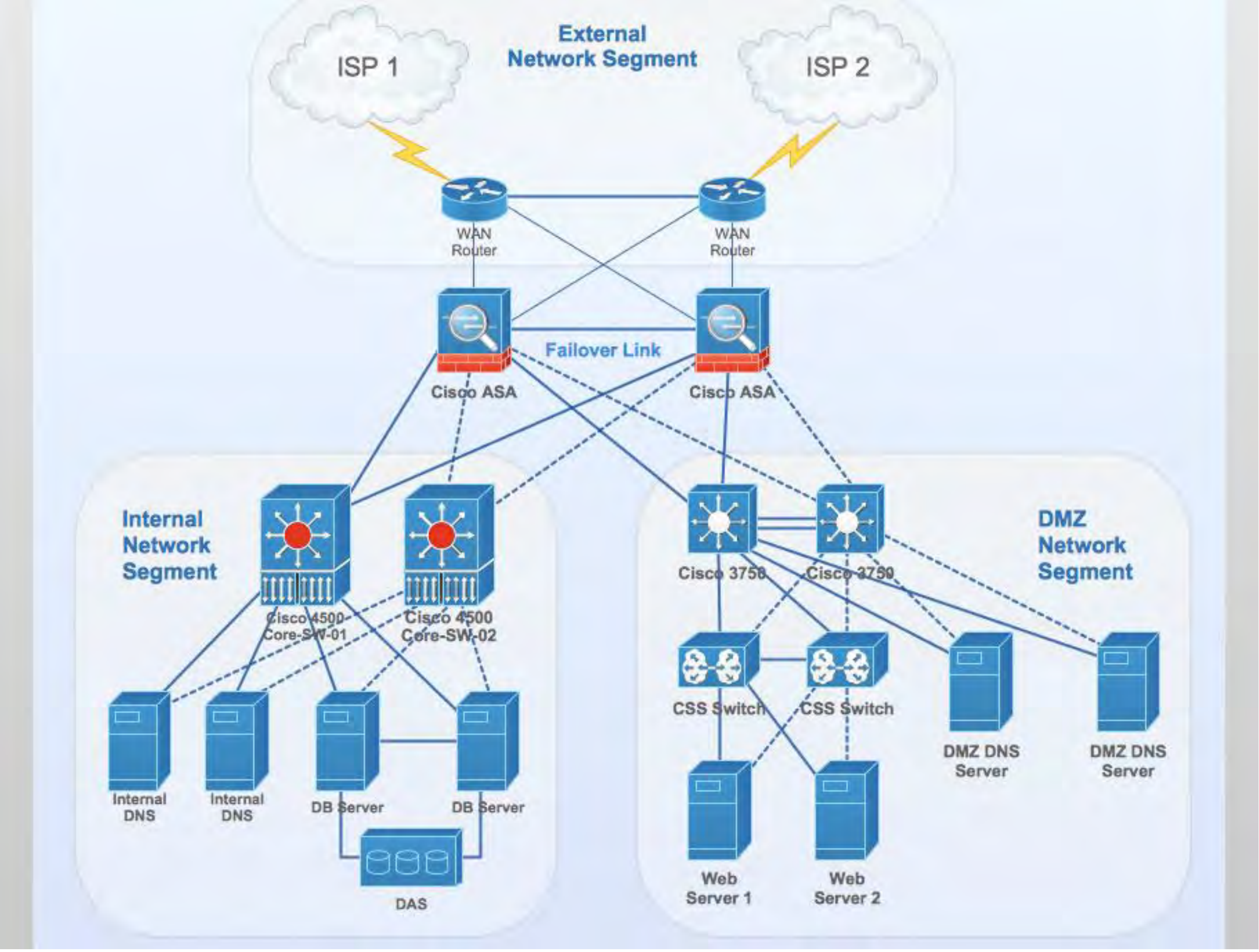
Usually the easiest way to represent a network

- Component connections remain the same, regardless of physical placement

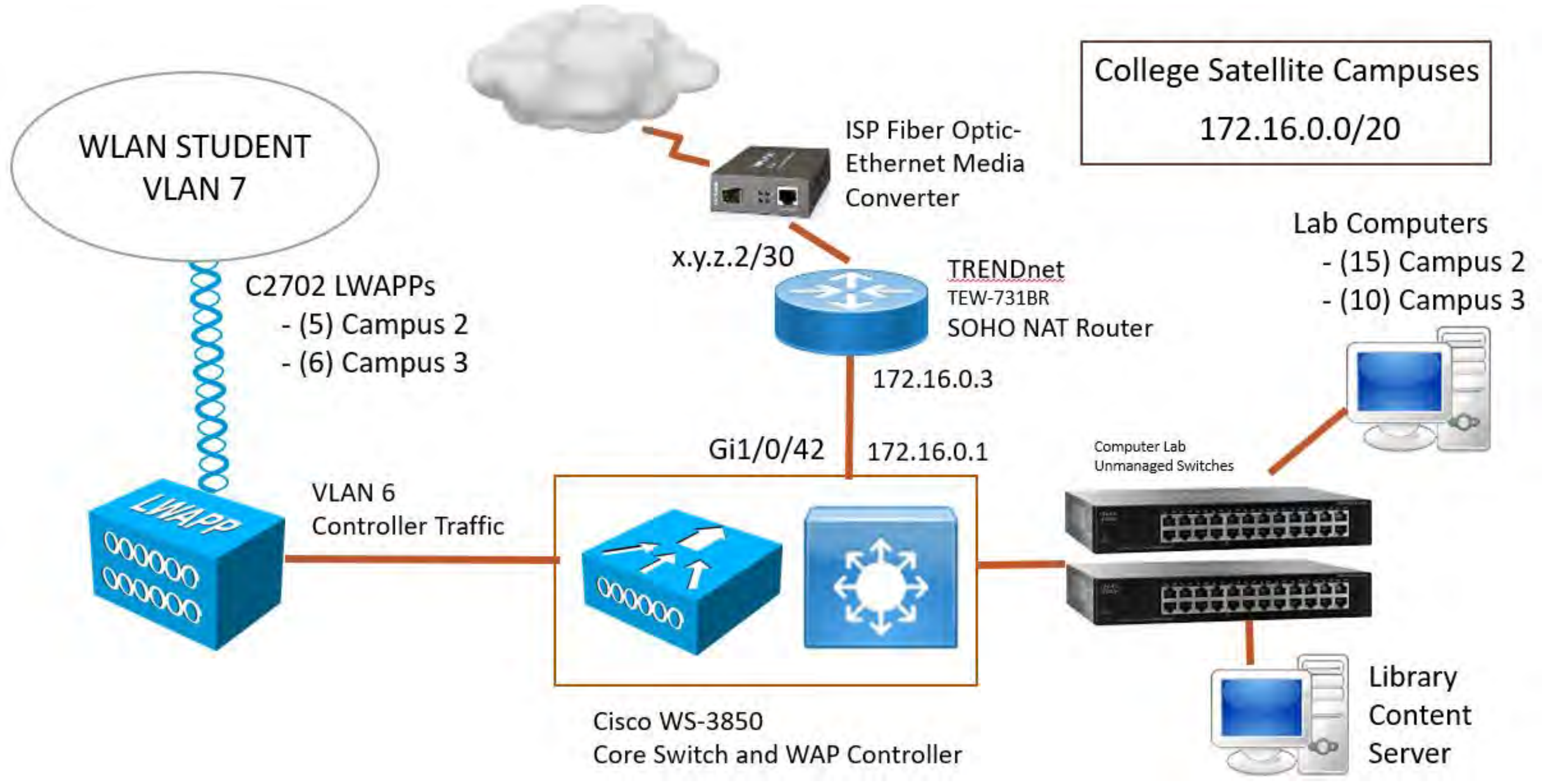
Technicians must deduce where devices or cabling are physically located

- Refer to other diagrams/documents for this information

Logical Network Diagram Example



Logical Network Diagram Example #2



ISP Fiber Optic-Ethernet Media Converter

TRENDnet
TEW-731BR
SOHO NAT Router

College Satellite Campuses
172.16.0.0/20

Lab Computers
- (15) Campus 2
- (10) Campus 3

Library Content Server

Cisco WS-3850
Core Switch and WAP Controller

Physical Network Diagram

Used by technicians to physically locate devices and cabling

If required, may be highly physically detailed

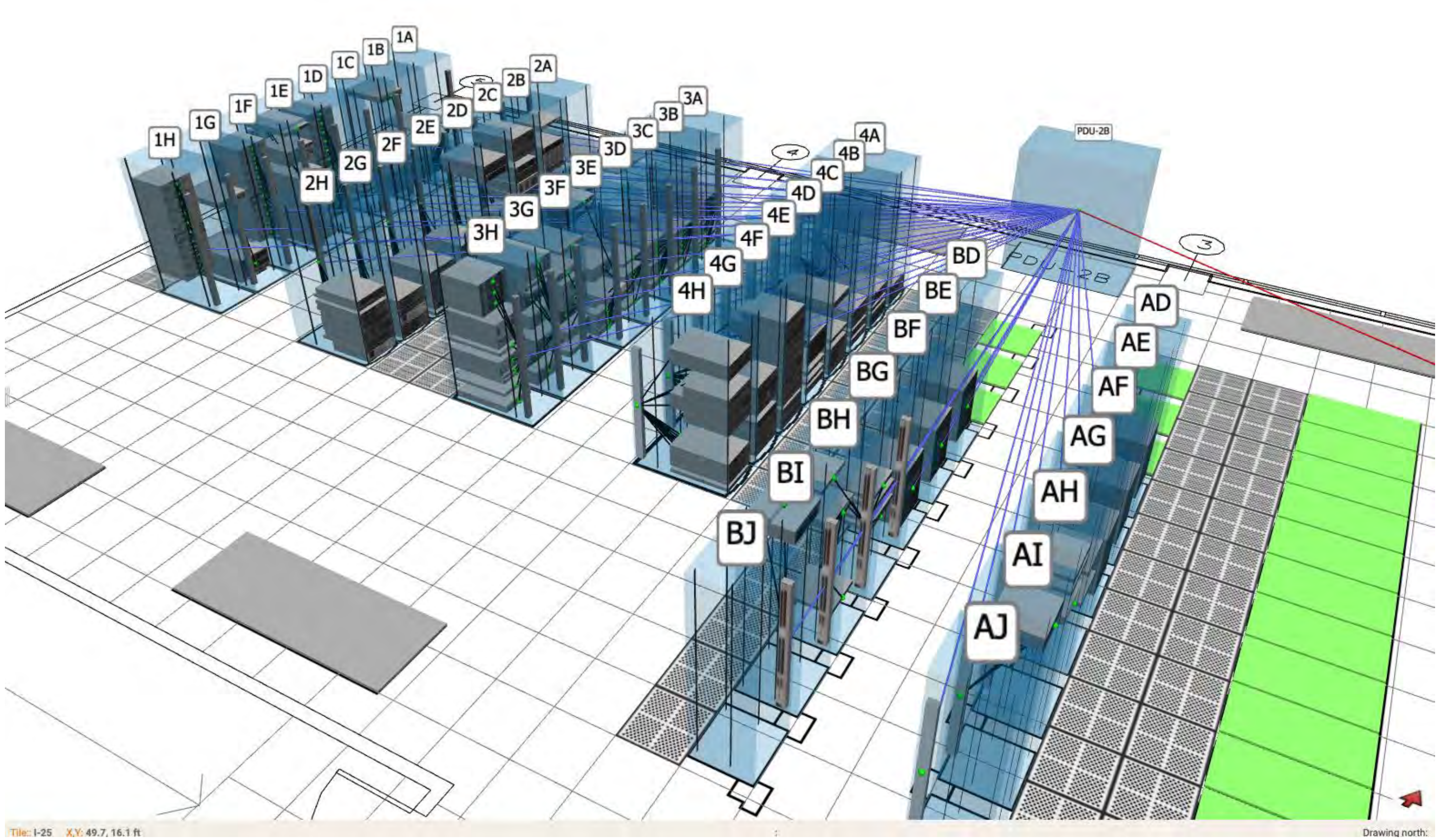
- May include precise measurements and exact connector types

Or may be partly "logical" for visual simplicity

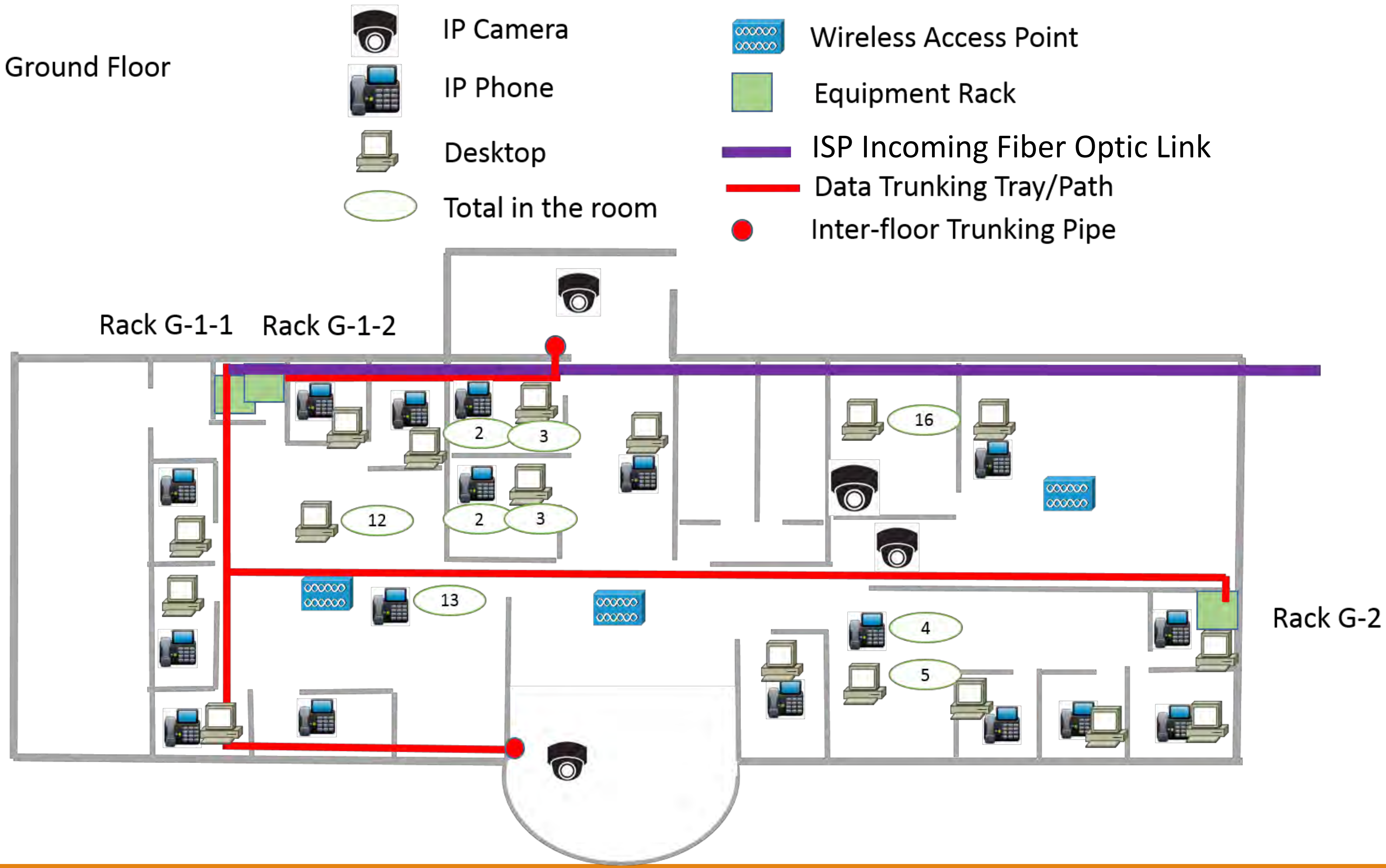
- May just show a "count" of desktop computers or phones in a room
- Devices should be easily located once the technician is in the room

A topology diagram is a type of physical diagram

Datacenter Physical Topology Example

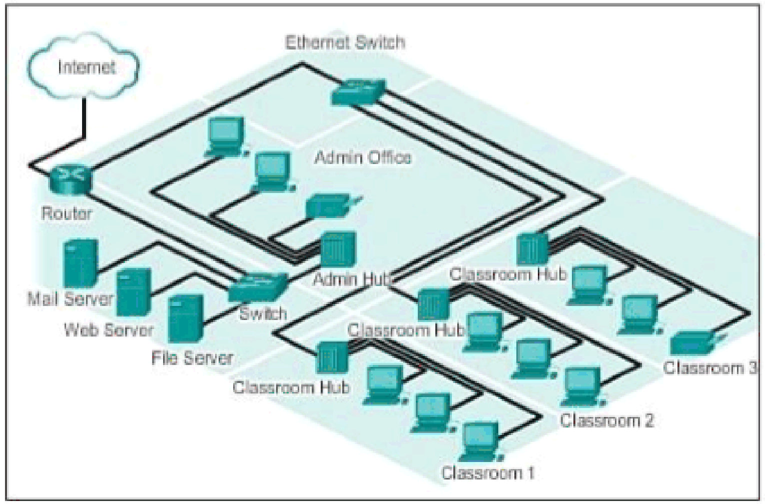


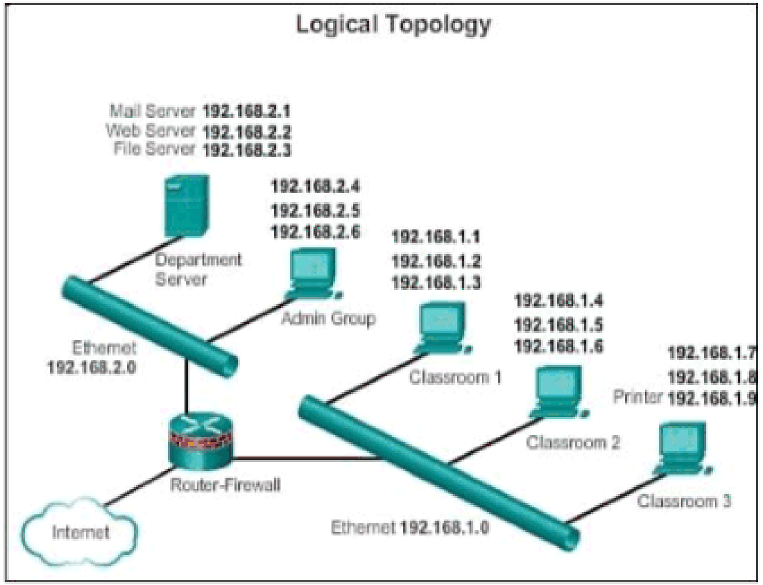
Simple Topology Diagram Example



Topology Comparison Example

Unless they are part of a floor plan, most physical topology diagrams are still partly logical





Physical Topology

is the physical layout of the components on the network

Logical Topology

determines how the hosts access the medium to communicate across the network

Rack Diagram

A type of physical diagram

Shows how computer and network equipment is organized in an equipment rack

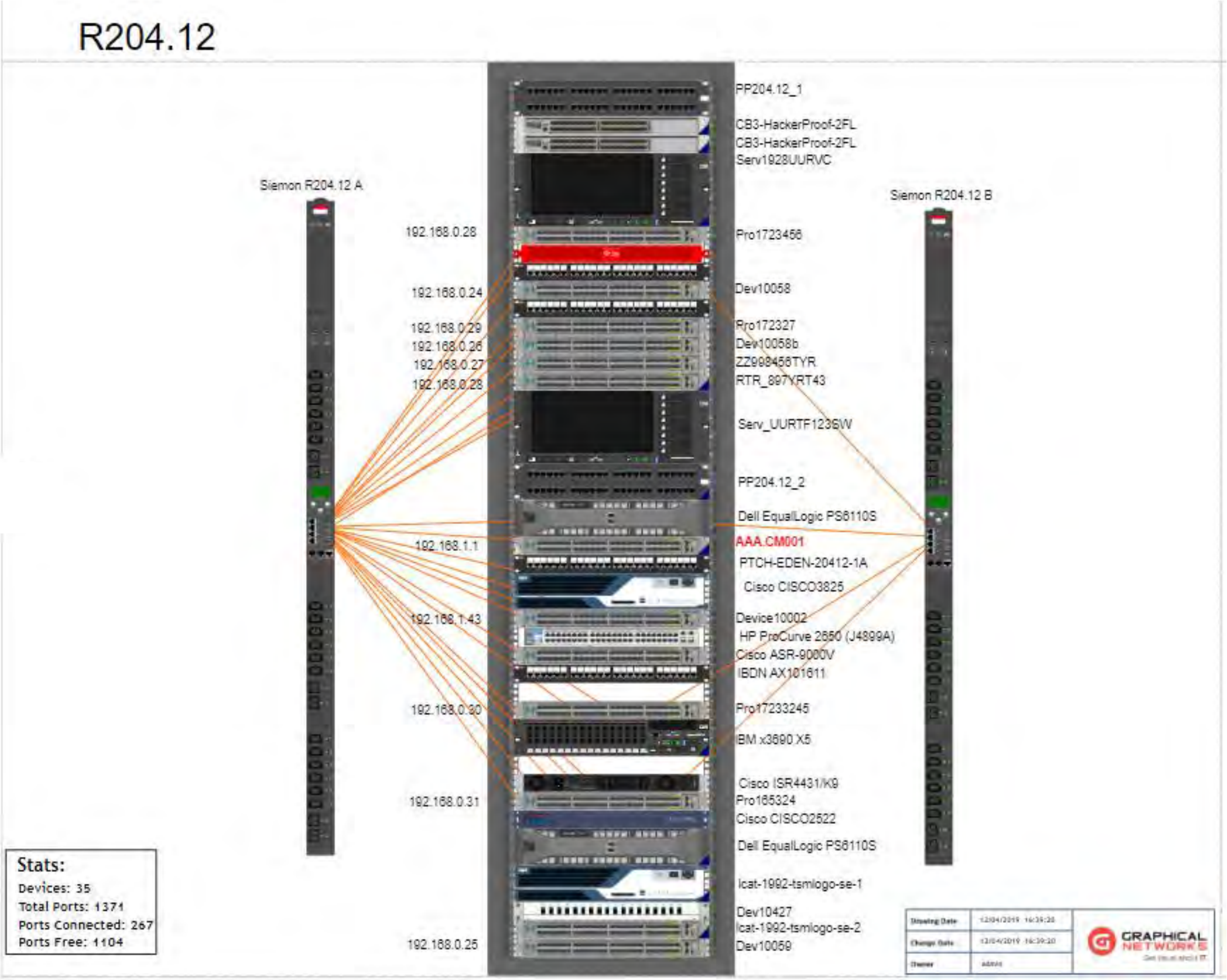
Visually simpler and “cleaner” than using a photo for documentation

Displays the location of each device

Often used to help designers/administrators visualize which racks to purchase and how to organize the equipment/cabling

Many vendors have software to help network administrators create the diagrams

Rack Diagram Example



Stats:
Devices: 35
Total Ports: 1371
Ports Connected: 267
Ports Free: 1104

Drawing Date	12/04/2019 16:39:20
Change Date	12/04/2019 16:39:20
Owner	admin

Wiring And Port Location Diagram

A physical topology diagram that shows where data and phone jacks are located in a room

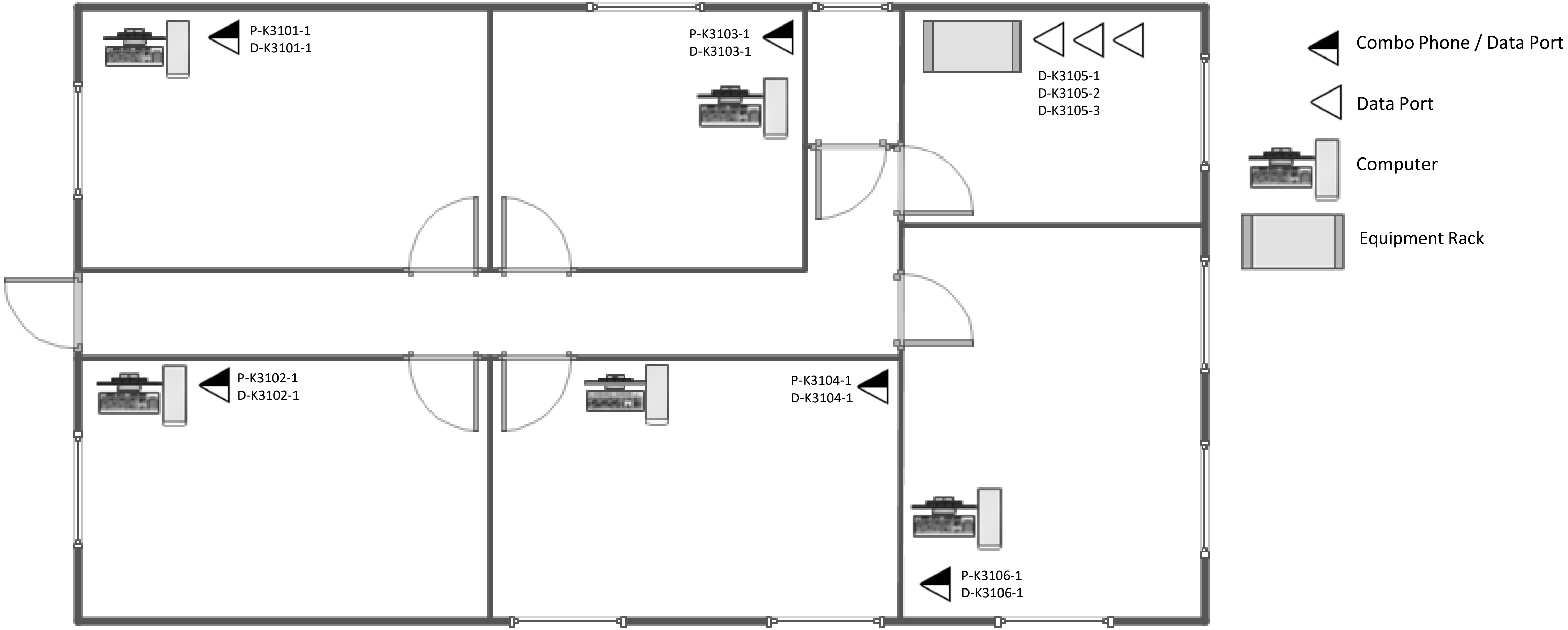
Used for both installation and troubleshooting

After installation, should be updated with port mapping labels

Might also show:

- Equipment placement (computer, phone, racks, printers, etc.)
- A/V equipment, ports and wiring
- Wireless access points and cameras
- Electrical outlets, switches, and lights

Port Location Diagram Example



Port Mapping Document

Typically a spreadsheet

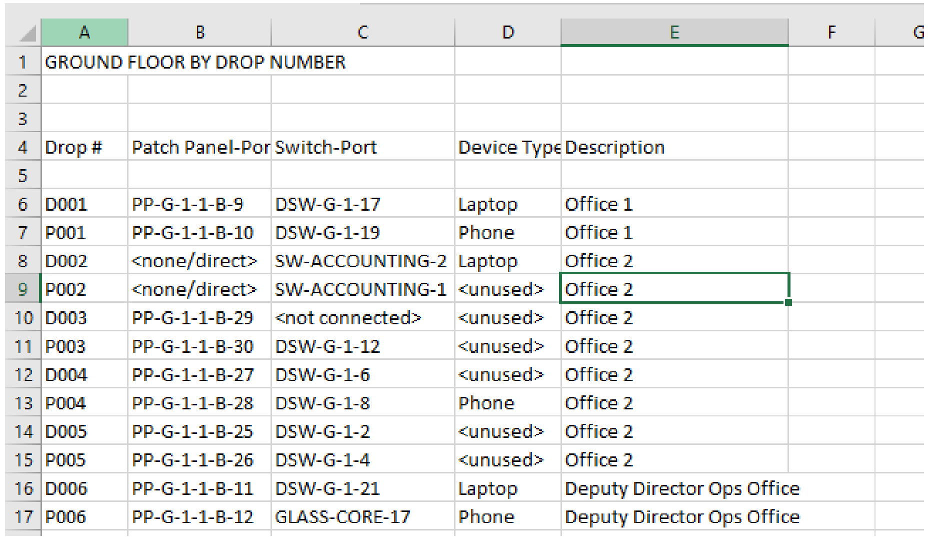
Maps patch panel ports to physical network drops (data and/or phone jacks)

May also map current connection of patch panel ports to switchports or other device ports

Allows a technician to quickly locate where a cable terminates, without having to trace it

Usually includes:

- Name/location of patch panel
- Patch panel port number
- Network jack location/number
- Cable number



	A	B	C	D	E	F	G
1	GROUND FLOOR BY DROP NUMBER						
2							
3							
4	Drop #	Patch Panel-Por	Switch-Port	Device Type	Description		
5							
6	D001	PP-G-1-1-B-9	DSW-G-1-17	Laptop	Office 1		
7	P001	PP-G-1-1-B-10	DSW-G-1-19	Phone	Office 1		
8	D002	<none/direct>	SW-ACCOUNTING-2	Laptop	Office 2		
9	P002	<none/direct>	SW-ACCOUNTING-1	<unused>	Office 2		
10	D003	PP-G-1-1-B-29	<not connected>	<unused>	Office 2		
11	P003	PP-G-1-1-B-30	DSW-G-1-12	<unused>	Office 2		
12	D004	PP-G-1-1-B-27	DSW-G-1-6	<unused>	Office 2		
13	P004	PP-G-1-1-B-28	DSW-G-1-8	Phone	Office 2		
14	D005	PP-G-1-1-B-25	DSW-G-1-2	<unused>	Office 2		
15	P005	PP-G-1-1-B-26	DSW-G-1-4	<unused>	Office 2		
16	D006	PP-G-1-1-B-11	DSW-G-1-21	Laptop	Deputy Director Ops Office		
17	P006	PP-G-1-1-B-12	GLASS-CORE-17	Phone	Deputy Director Ops Office		

Wiring Diagram

Generic term that shows how electrical or electronic devices are connected together

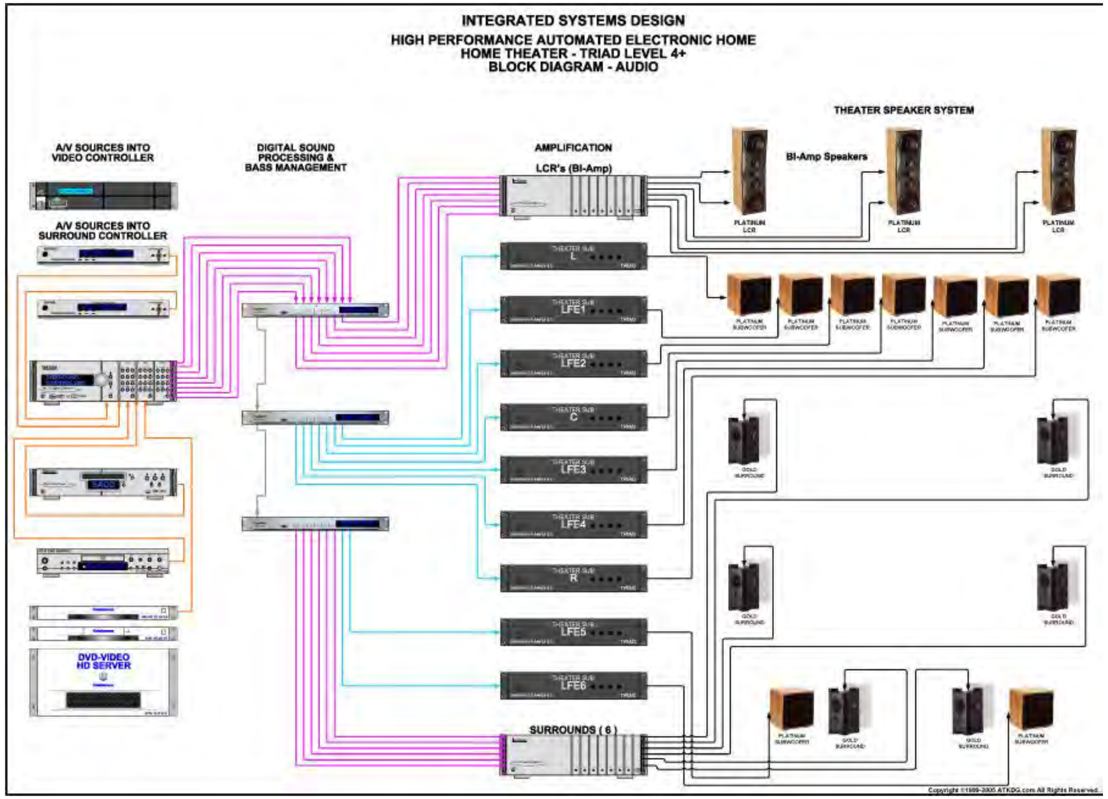
Simplified pictorial representation of an electrical circuit

Authoritative reference for installation and troubleshooting

Can be for high voltage or low voltage systems

Often used for:

- Audio/Visual systems
- Alarm/camera/security systems
- Lighting, HVAC, motors and other electrical systems



Floor Plan

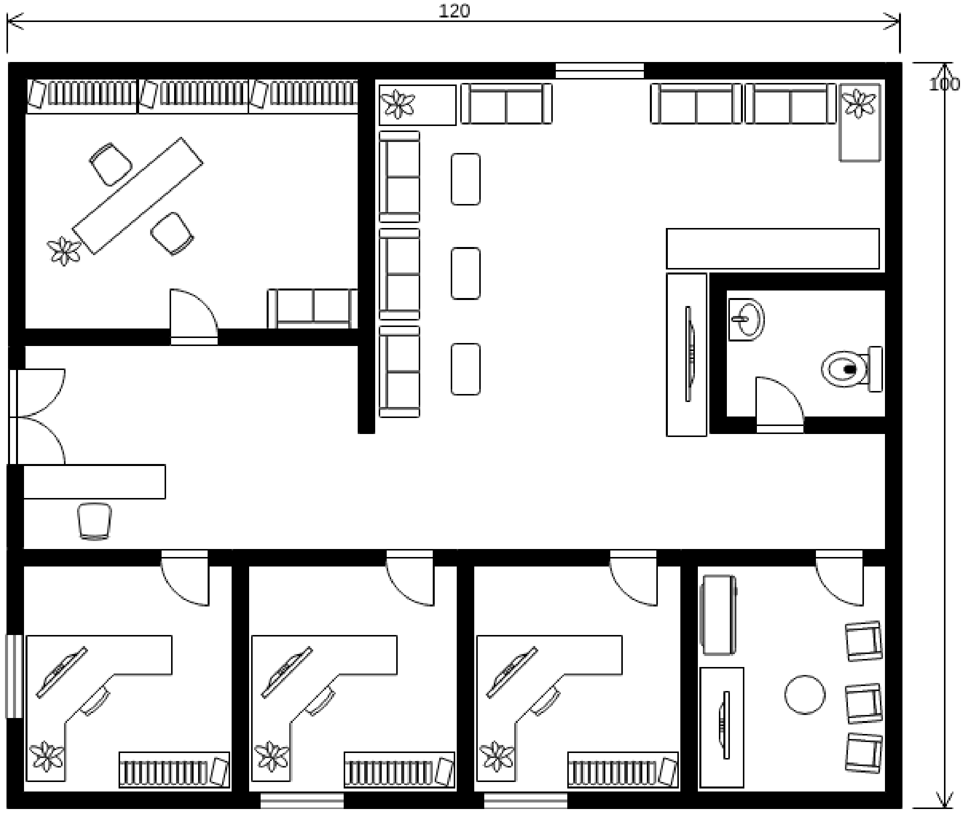
A scale diagram of the arrangement of rooms in one story of a building

View is from above

Shows location of hallways, walls, doors, furniture, appliances, stairs, elevator shafts, equipment, etc.

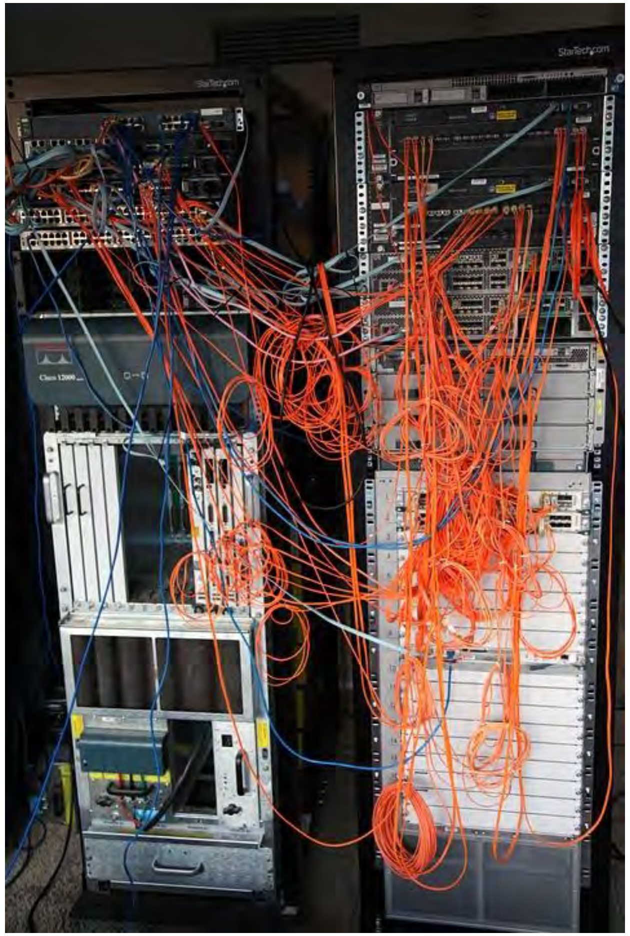
Shows in what direction doors open

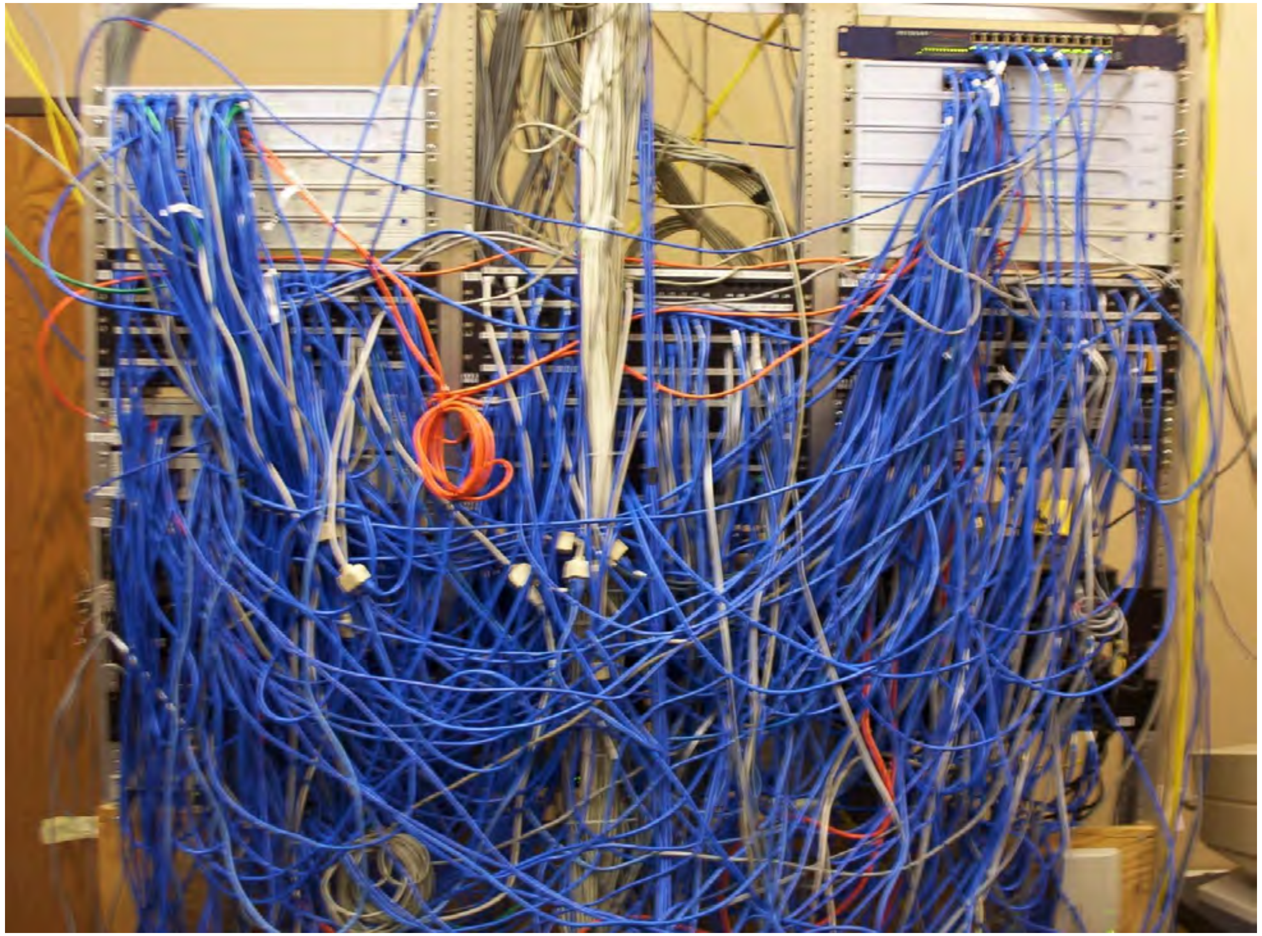
Usually includes exterior dimensions



Structured Cabling MDF and IDF

The Need for Cable Management





Images courtesy Pixabay & Wikimedia

Structured Cabling

A building or campus cabling infrastructure that that is organized into standardized structured elements

Standardization provides identical environments at all facilities

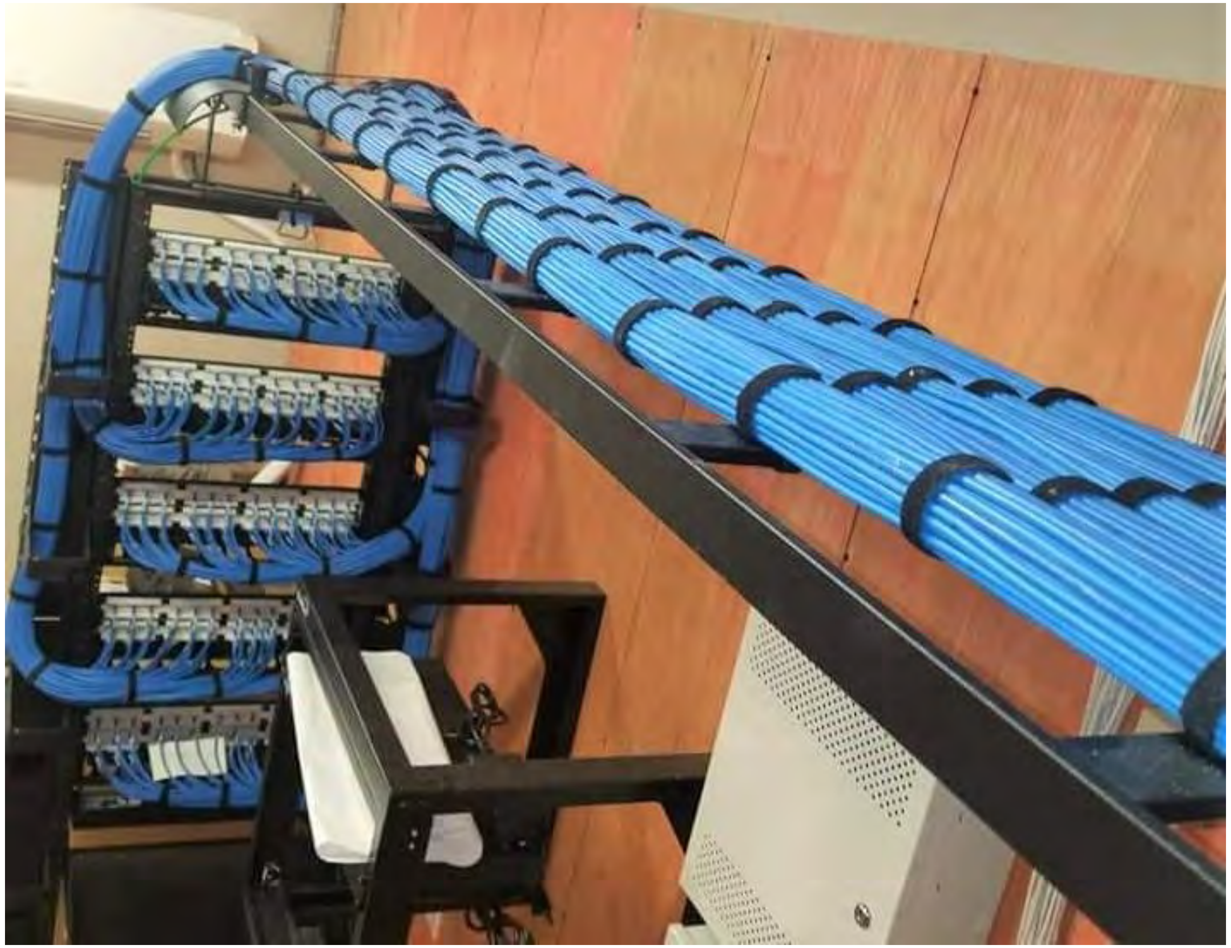
- Easier to document
- Easier to modify or expand
- Consistent performance
- Facilitates maintenance and troubleshooting
- Consistency helps manage complexity

Structured cabling can included:

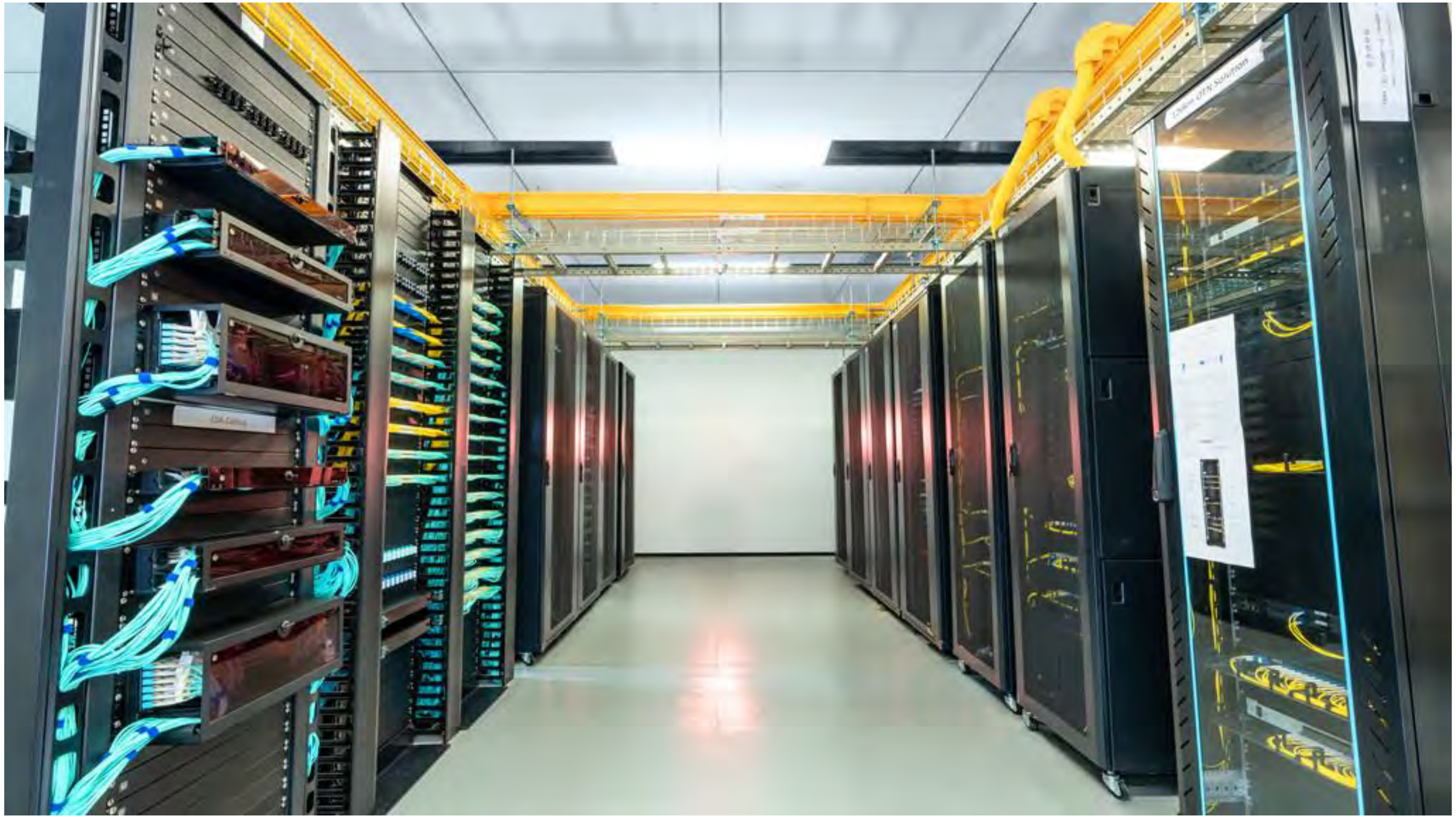
- MDF and IDF
- Horizontal and vertical cabling
- Entrance facility (where telco lines come in)
- Equipment room
  - has patch panels to IDFs and incoming telco cabling
  - may also house routers, servers, PBX, switches, etc.
- Work area (where end users work)

Top of Rack (ToR) is an example of structured cabling

Structured Cabling Example



Structured Cabling Example #2



Main Distribution Frame (MDF)

The core part of a structured cabling system

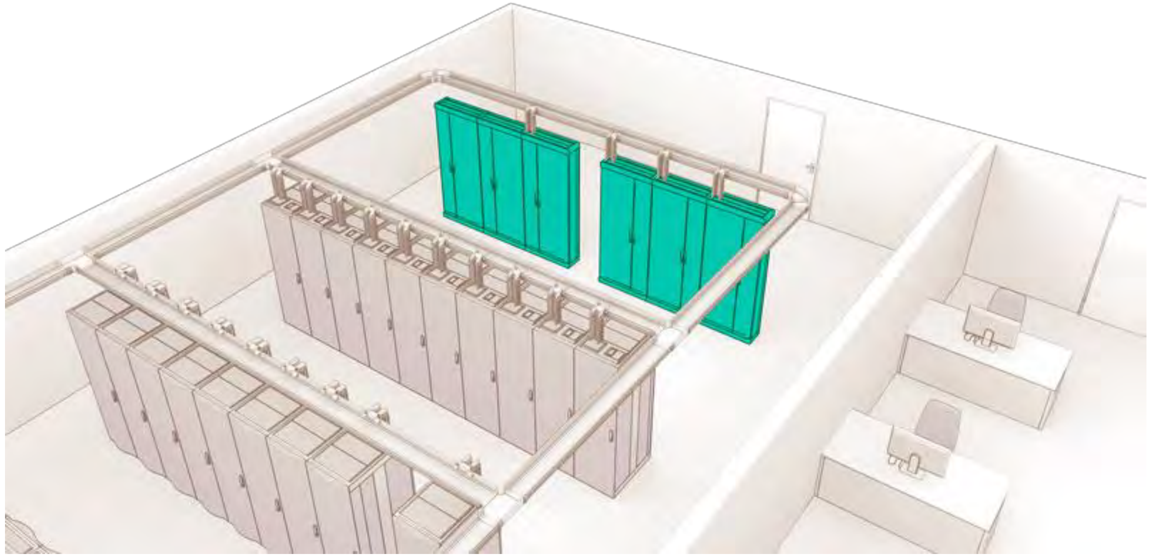
Located in the Main Distribution Area of a datacenter

Contains:

- Backbone cabling to IDFs and other buildings
- Incoming telco/ISP links and demarcs

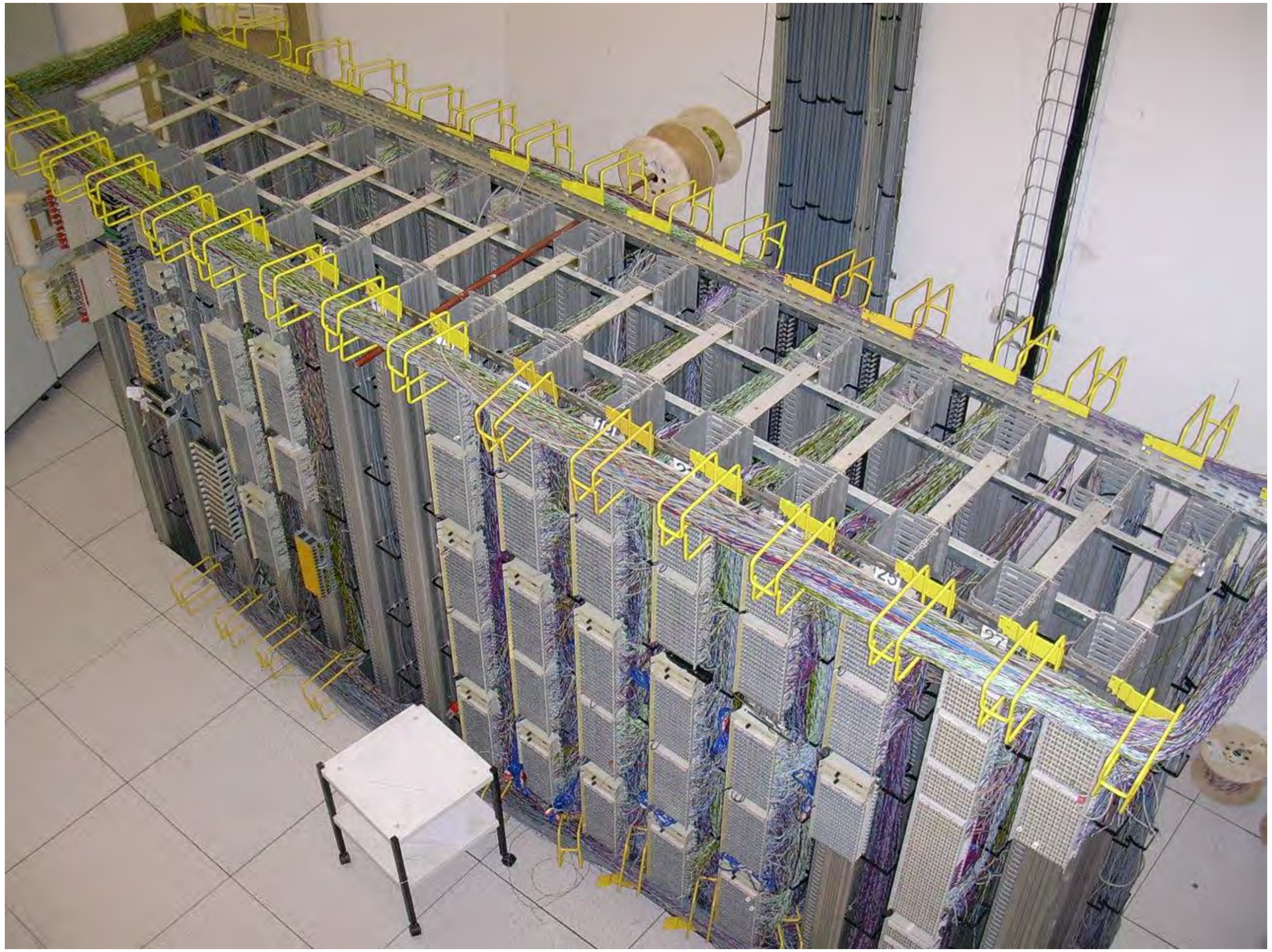
Traditionally referred to a local telephone exchange where local loops were terminated and patched to telco equipment

Now refers to the main nerve center of a datacenter



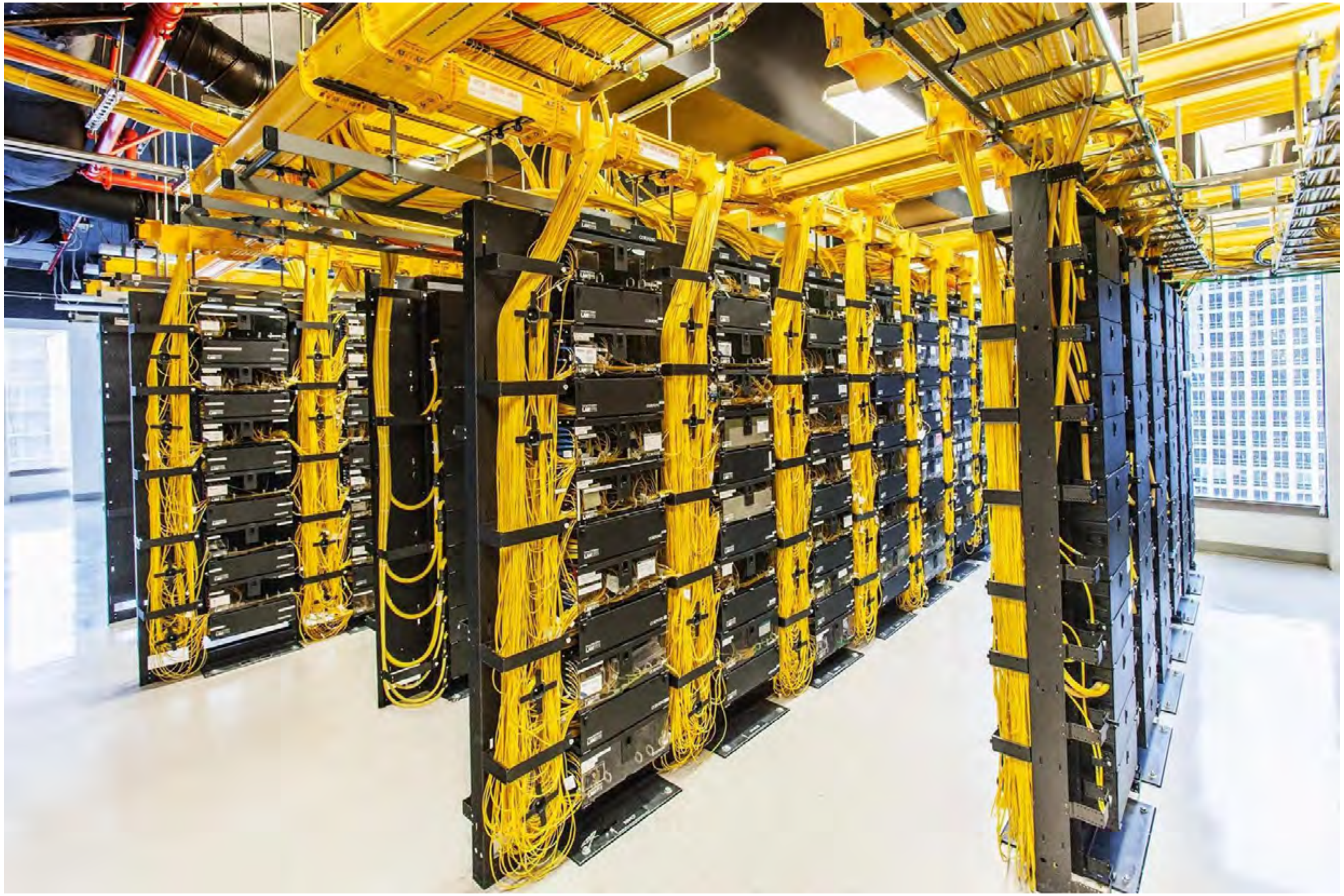
Note: A “frame” is one or more equipment cabinets connected to each other

Telco MDF Example



By YannTech at French Wikipedia, CC BY-SA 2.5, https://commons.wikimedia.org/w/index.php?curid=12584353

Datacenter Fiber Optic MDF Example



MDF Physical Topology Diagram Example

Fault-tolerant dual MDFs
with backup frames

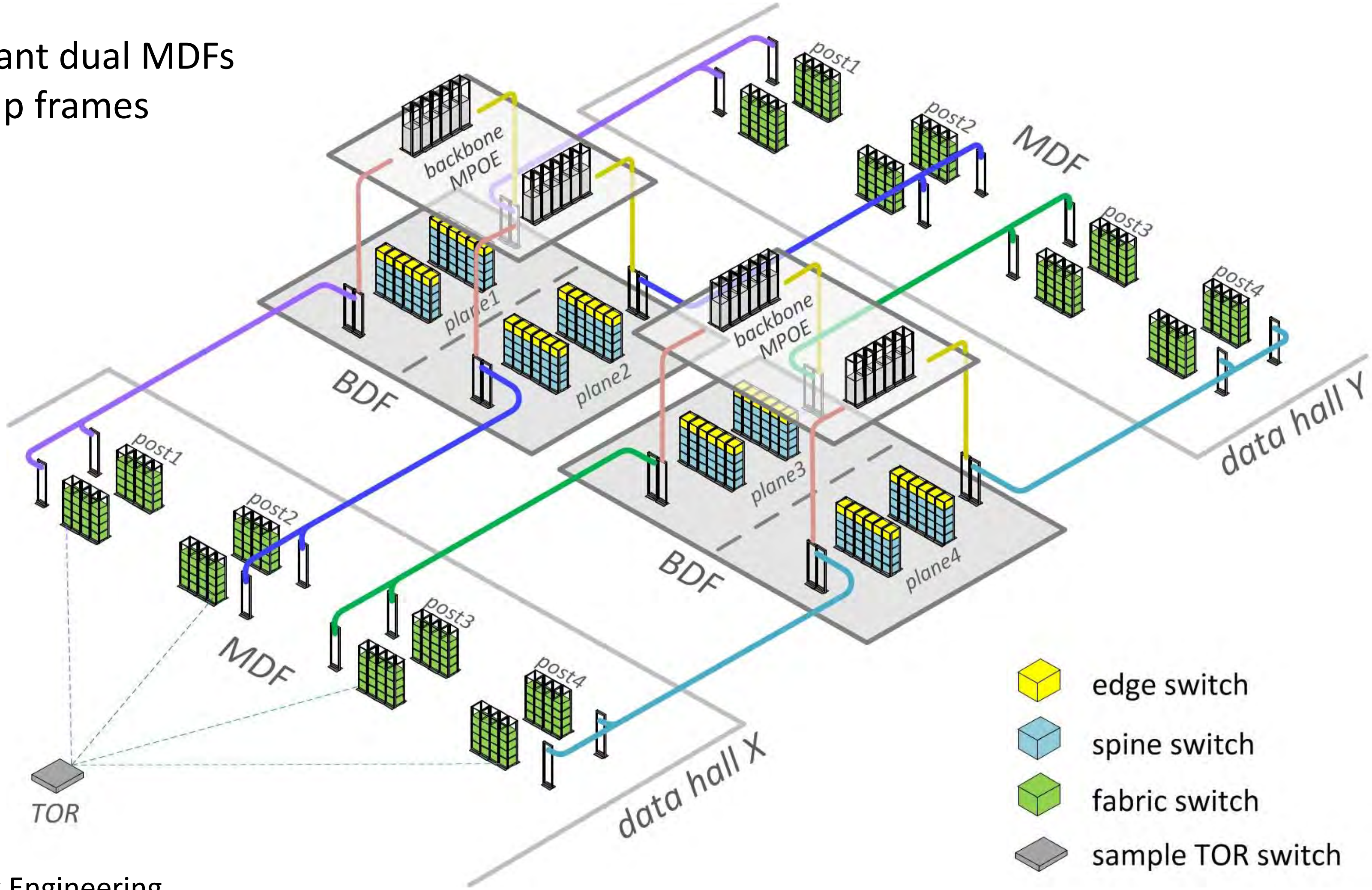


Image courtesy Facebook Engineering

Intermediate Distribution Frame (IDF)

Smaller version of MDF

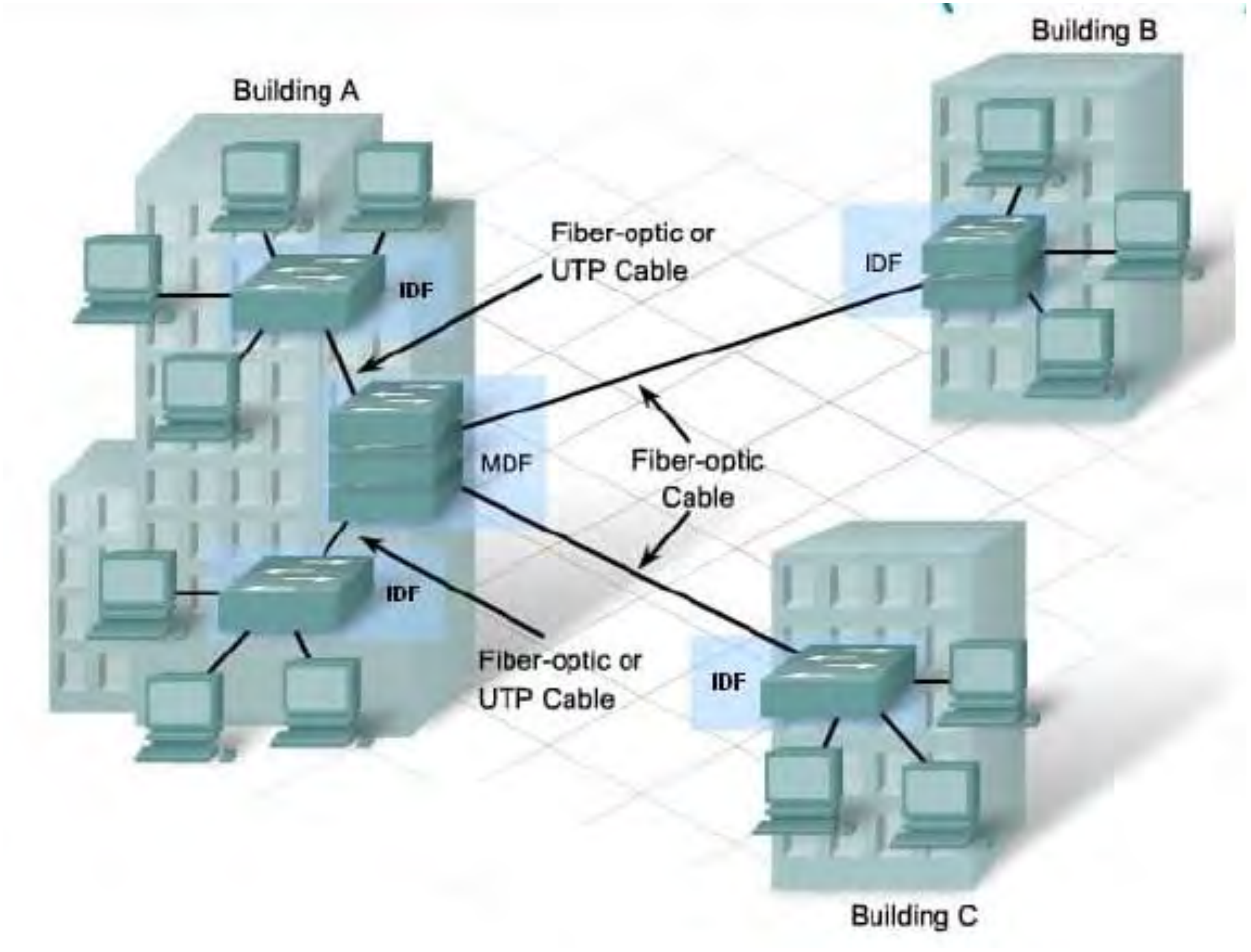
Usually covers part of a building (one or more floors)

Can be one rack in a wiring closet or a room full of racks

Connects to user work areas

Likely to include distribution layer switches

MDF and IDF Relationship Example



MDF and IDF Documentation

Part of the overall collection of network documentation

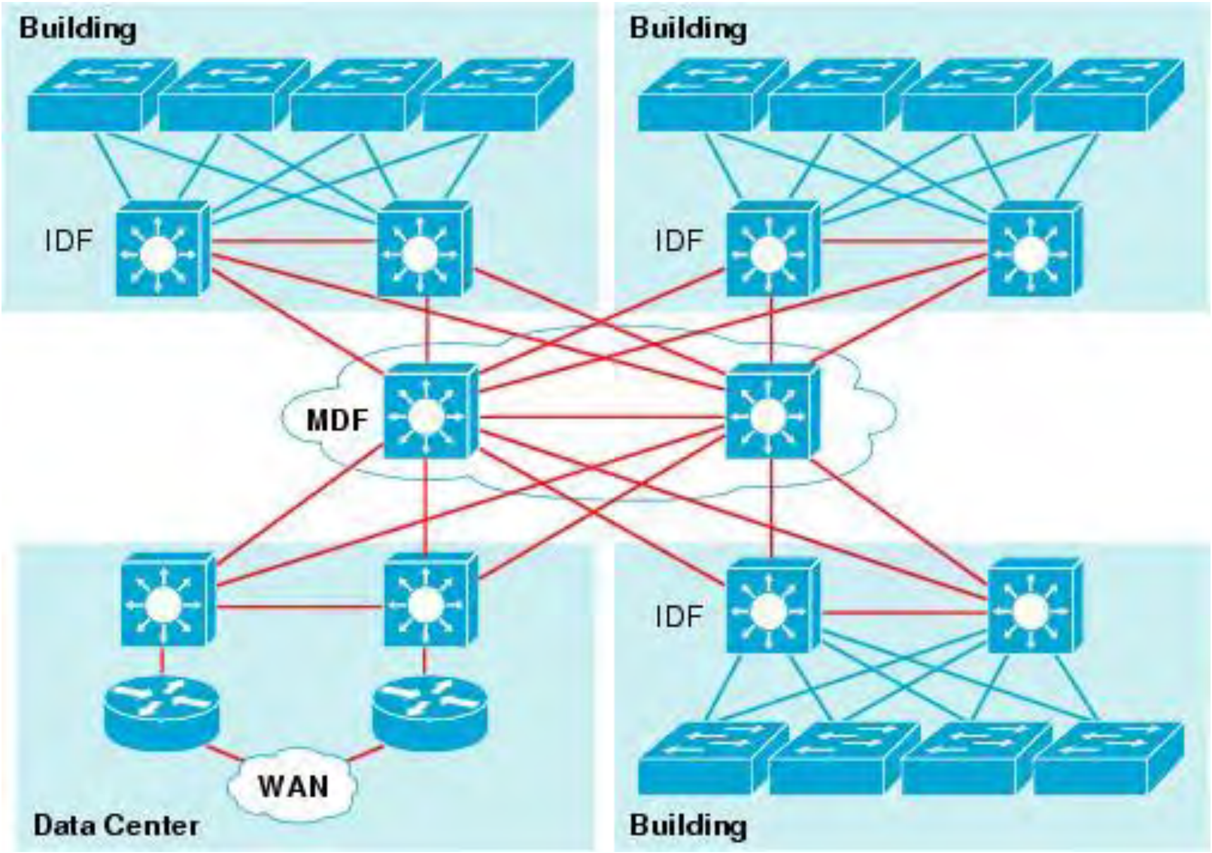
Documentation for the MDF and IDFs will include:

Logical network diagram(s)

Physical network / rack diagram(s)

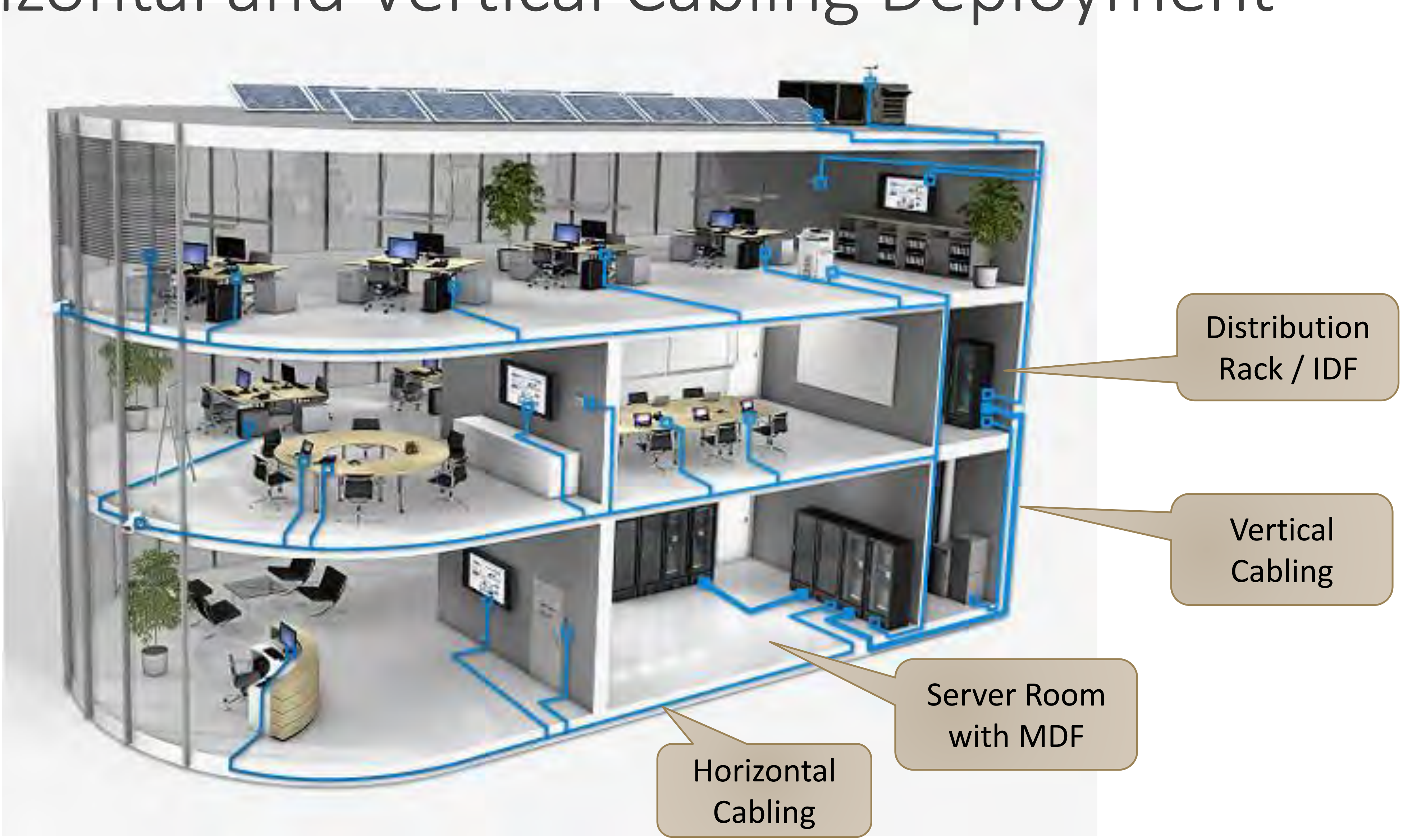
Patch panel and switch port mapping documents

MDF and IDF Logical Diagram Example



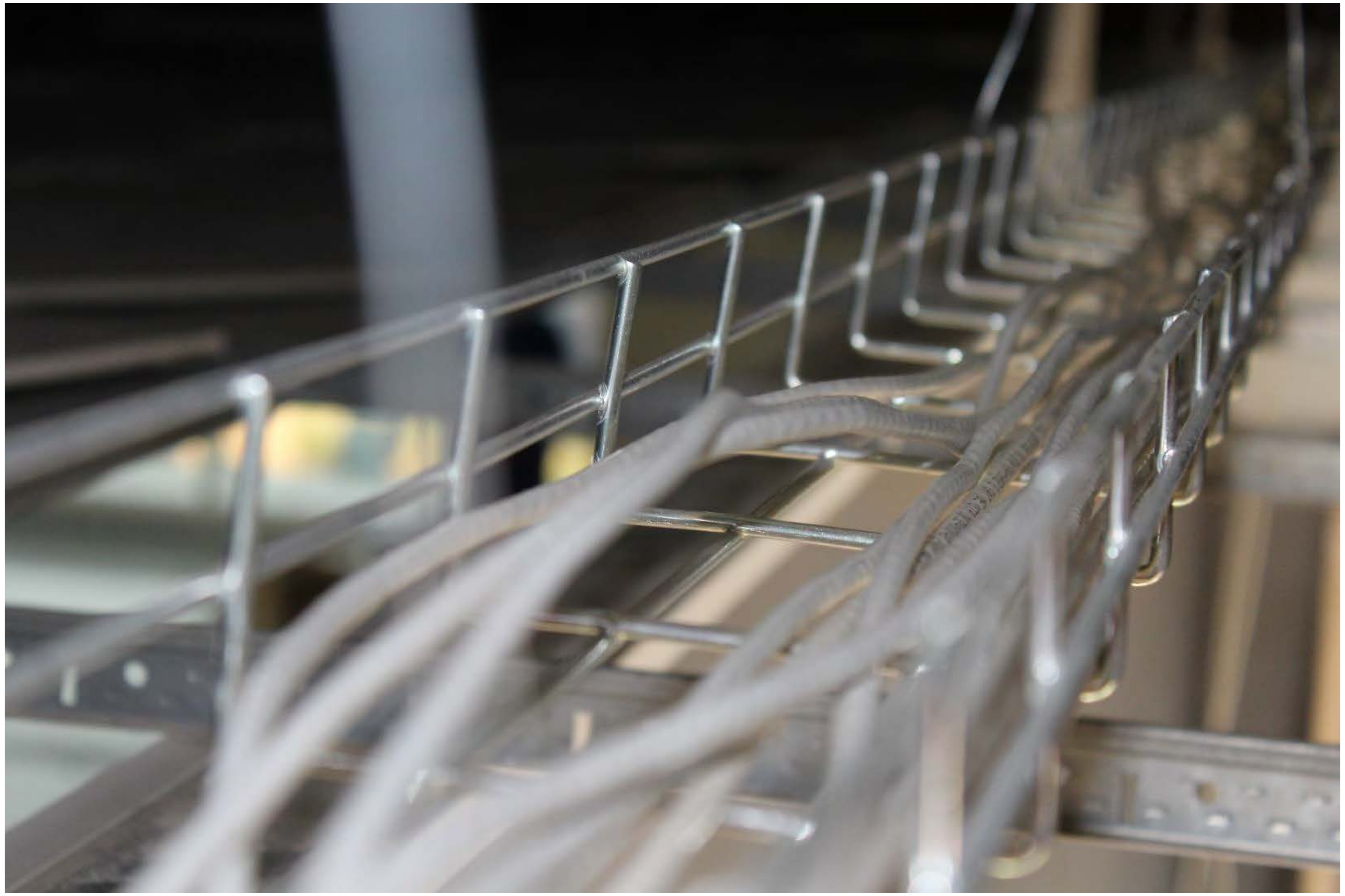
Horizontal and Vertical Cabling

Horizontal and Vertical Cabling Deployment



Horizontal Cabling Example

Horizontal Cabling Example #2



Horizontal Cabling Under Floor Example

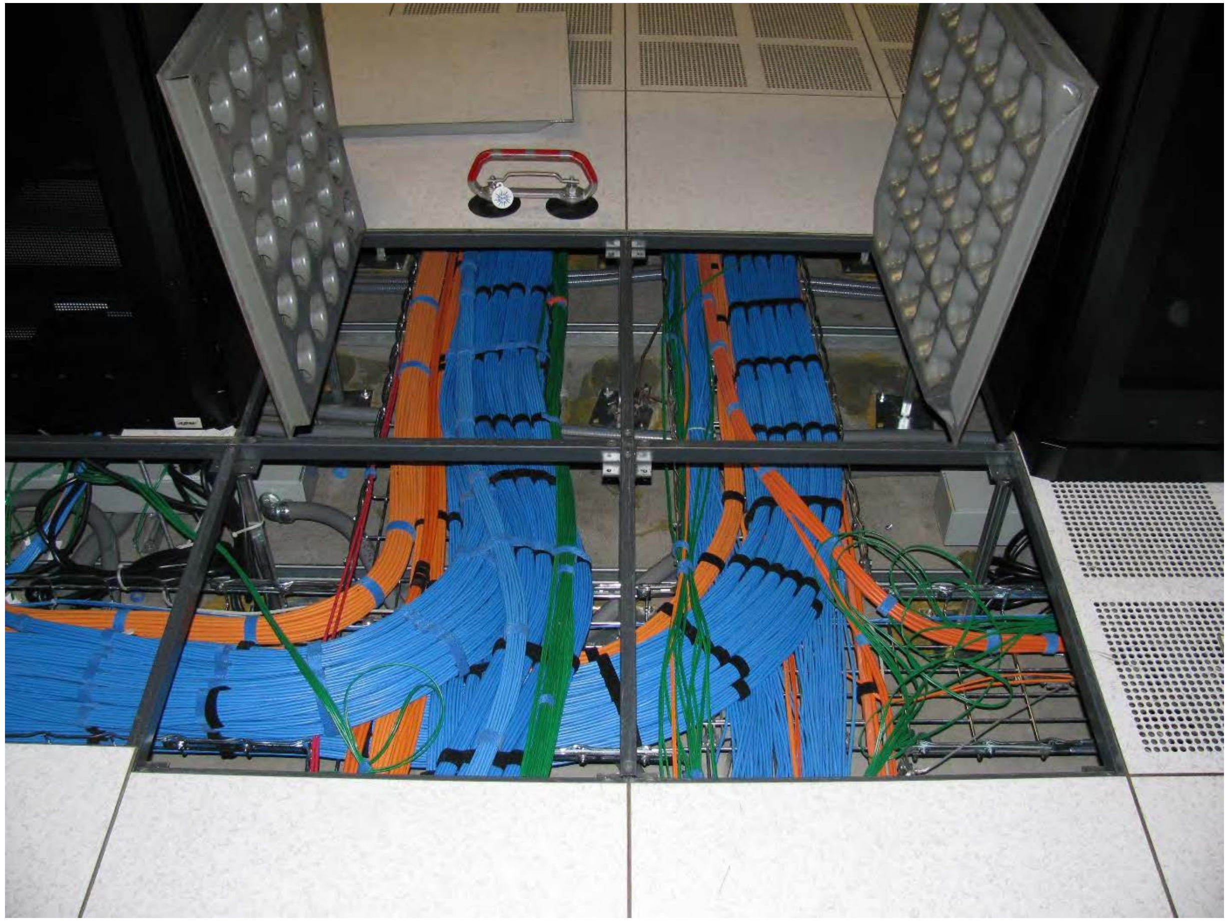
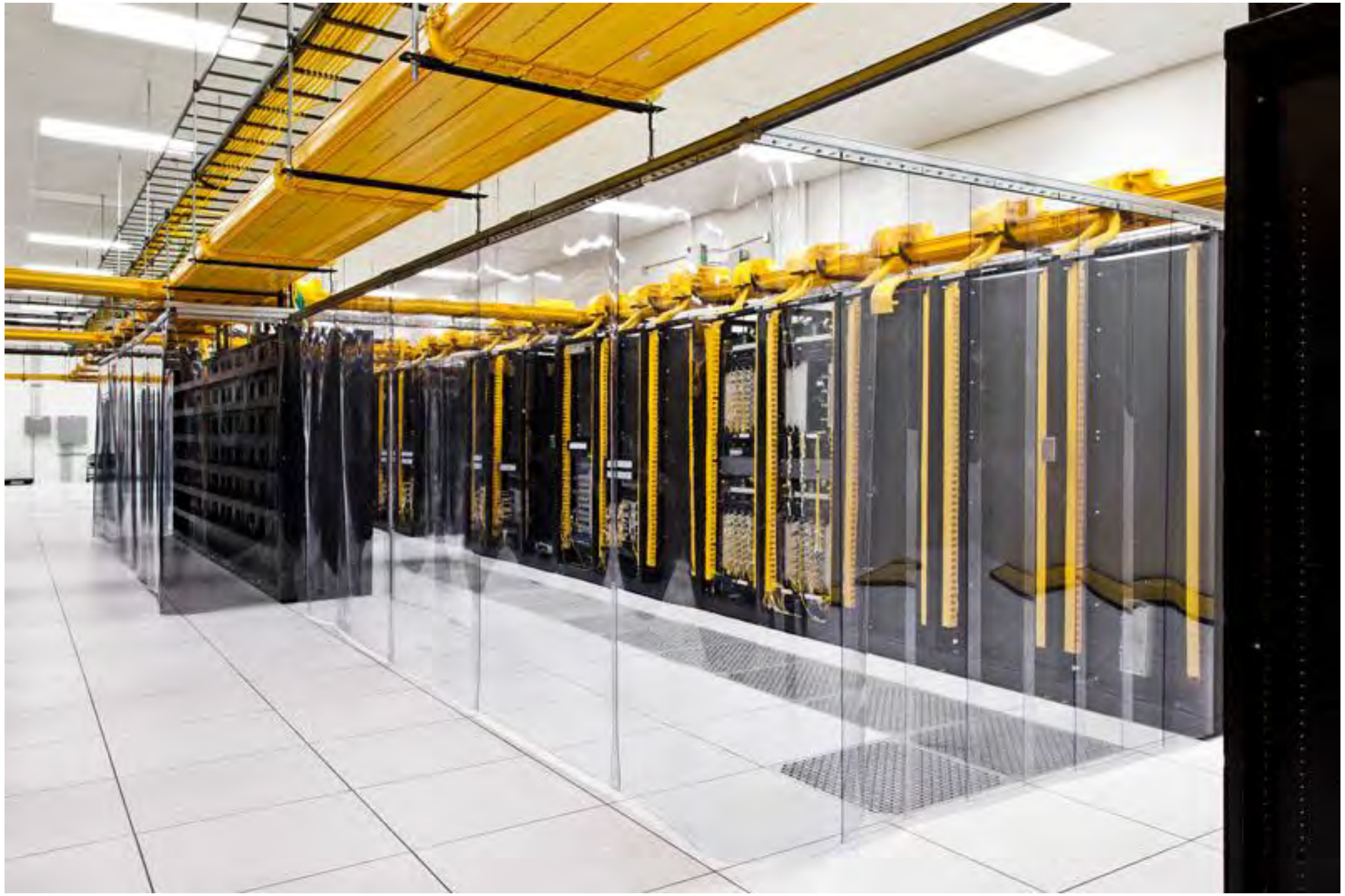


Image courtesy Wikimedia

Horizontal Cabling Above Datacenter Racks



Vertical Cabling

Cabling is usually secured to a ladder/cable rack

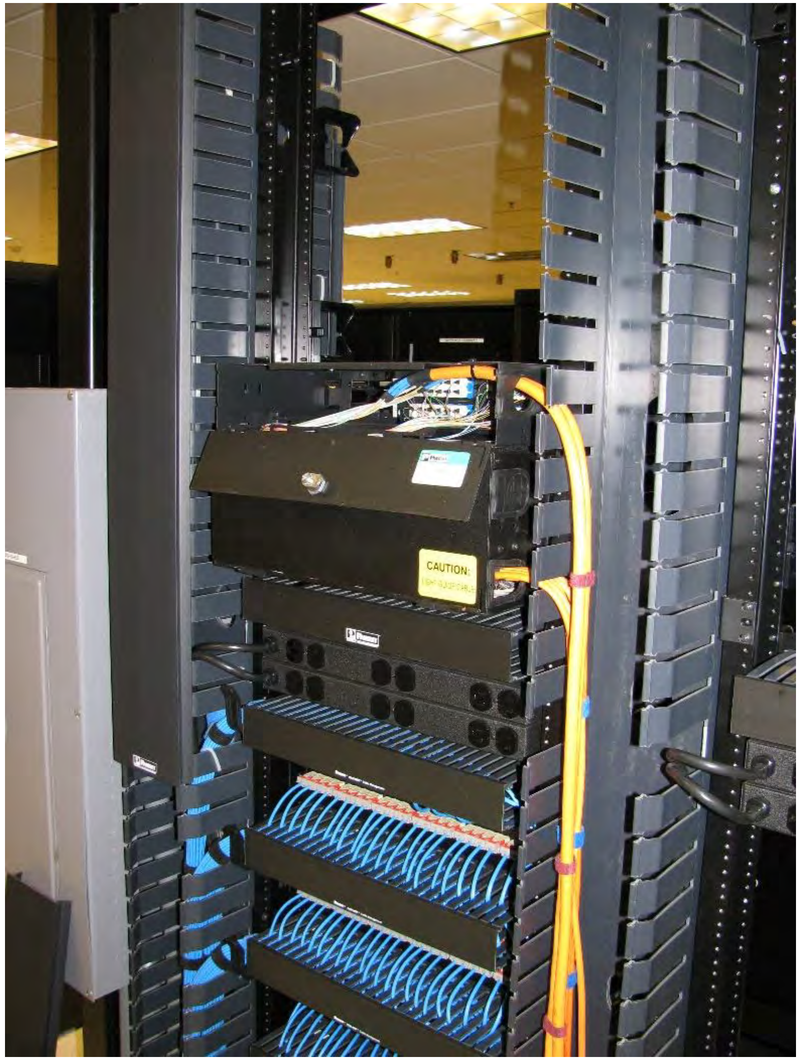
Secure the cabling at frequent intervals

“Comb” the cabling before bundling it

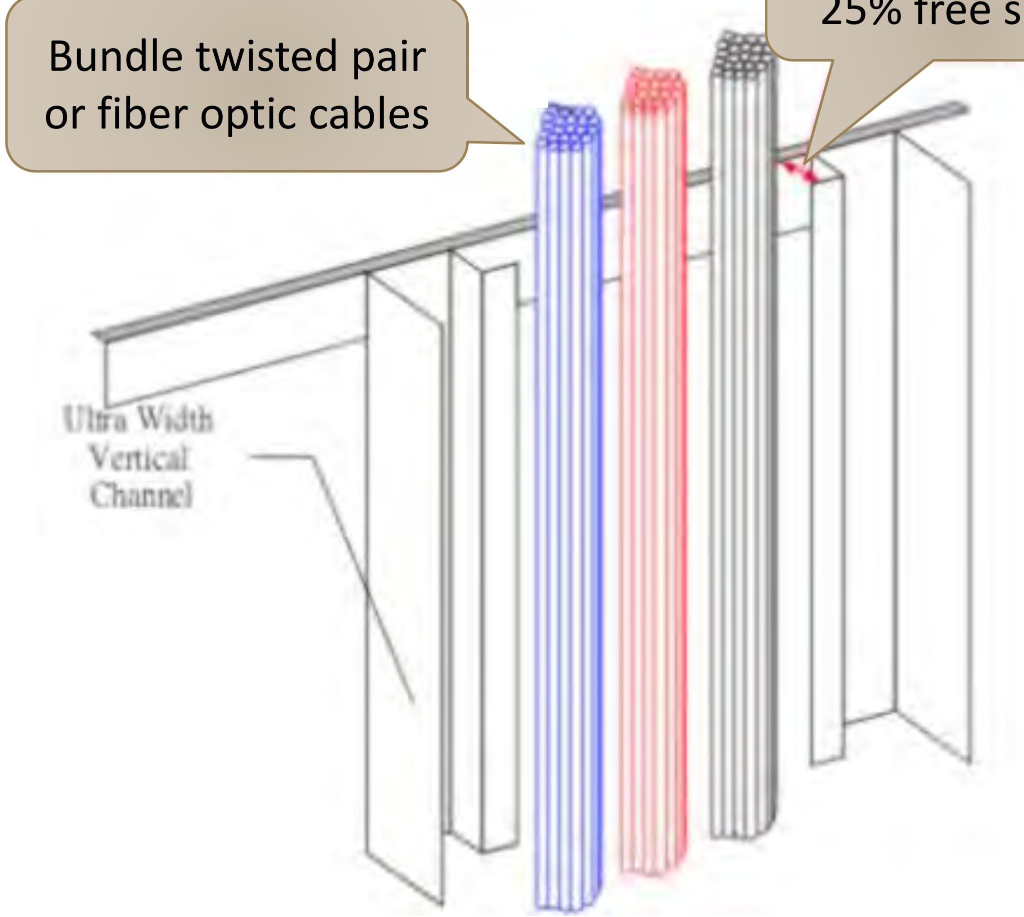
Especially important to strain relief the cable

If cabling is delicate, use Velcro as opposed to zip ties

Or wrap a strain relief “skin” around the cable before zip tying it to the rack



Using a Vertical Cable Rack



Bundle twisted pair or fiber optic cables

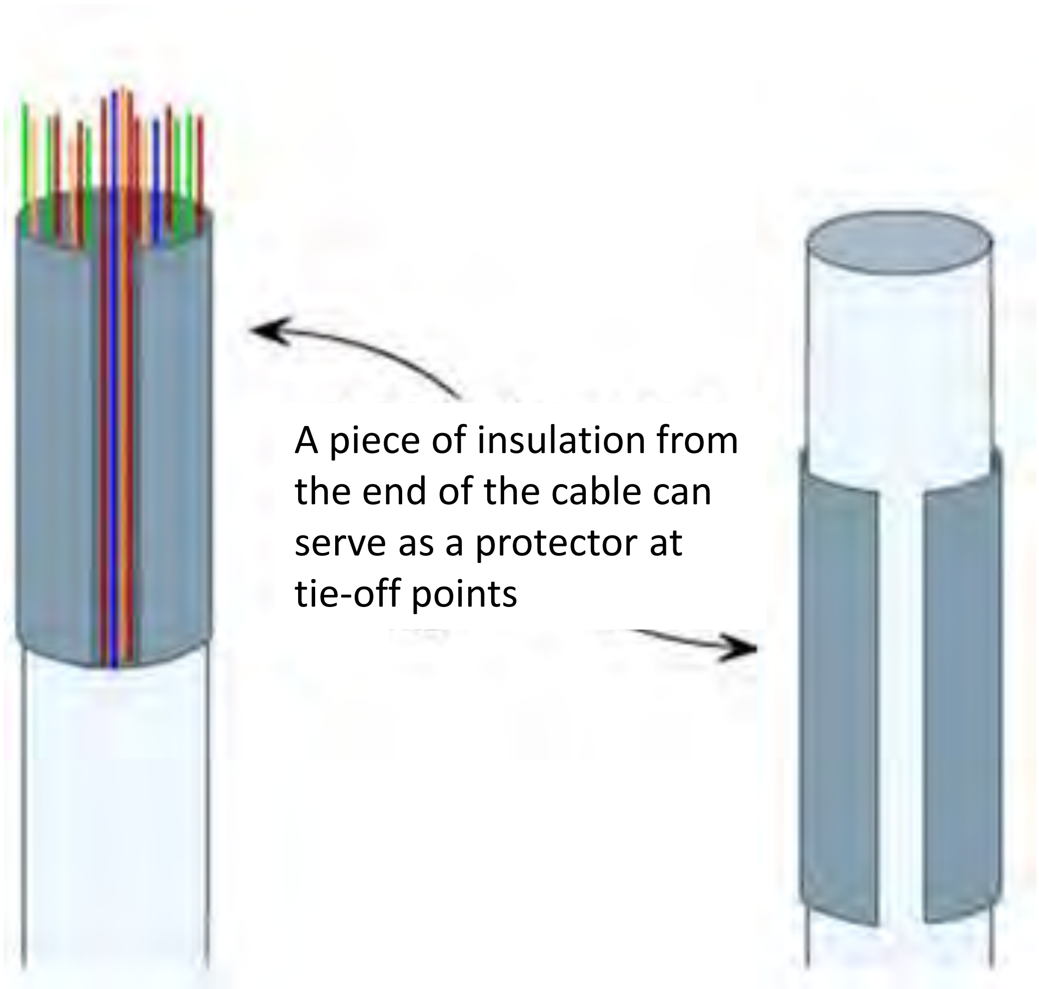
Leave about 20 – 25% free space

Fiber Optic Vertical Cable Strain Relief

Remove a small section of sheathing from the end of the cable

Use that “skin” to wrap around the outside of the cable to provide double-sheathing

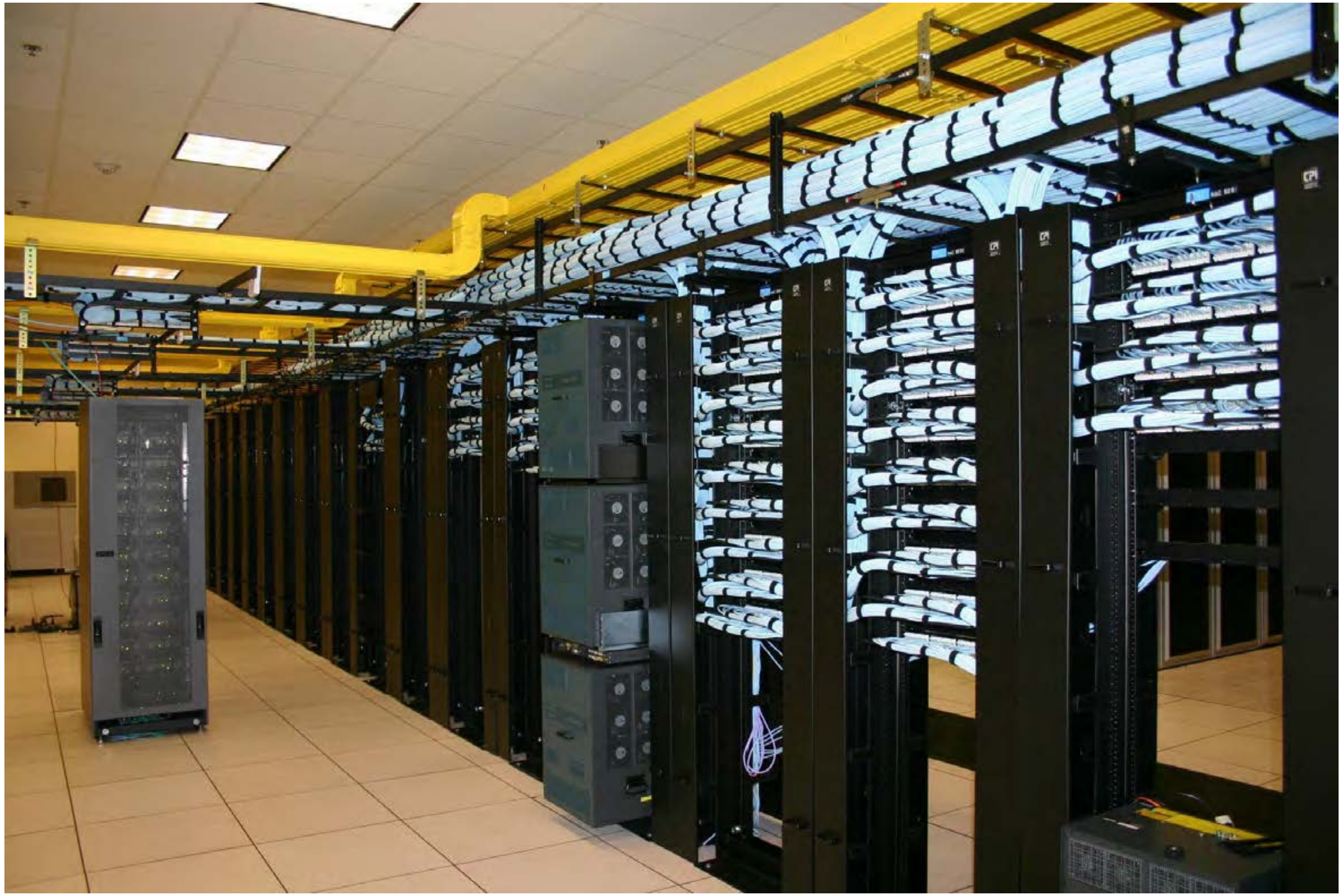
You can also use a fiber optic cable skin to wrap multiple CAT 5/6/7 etc. cables



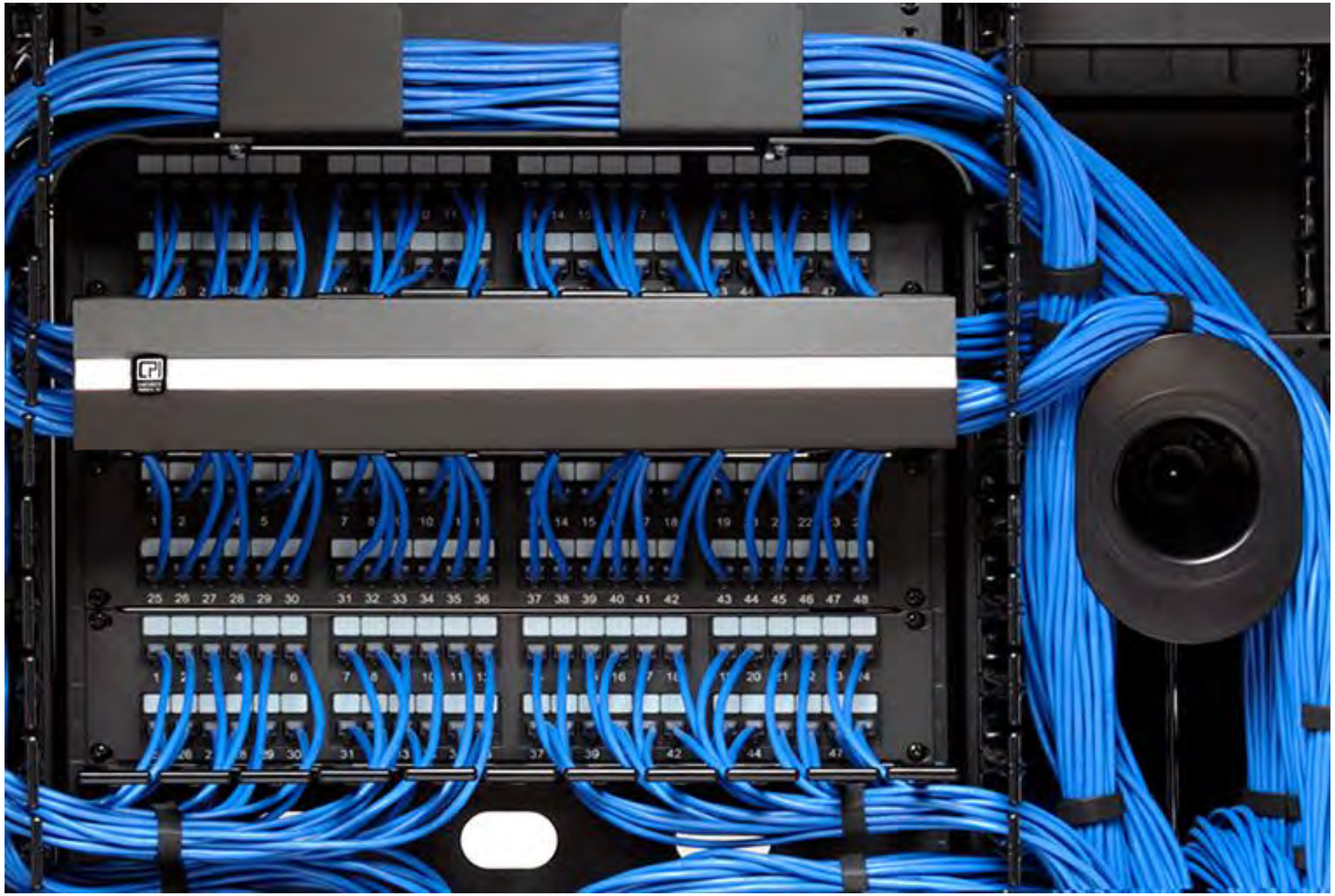
A piece of insulation from the end of the cable can serve as a protector at tie-off points

Vertical Cable Support Examples

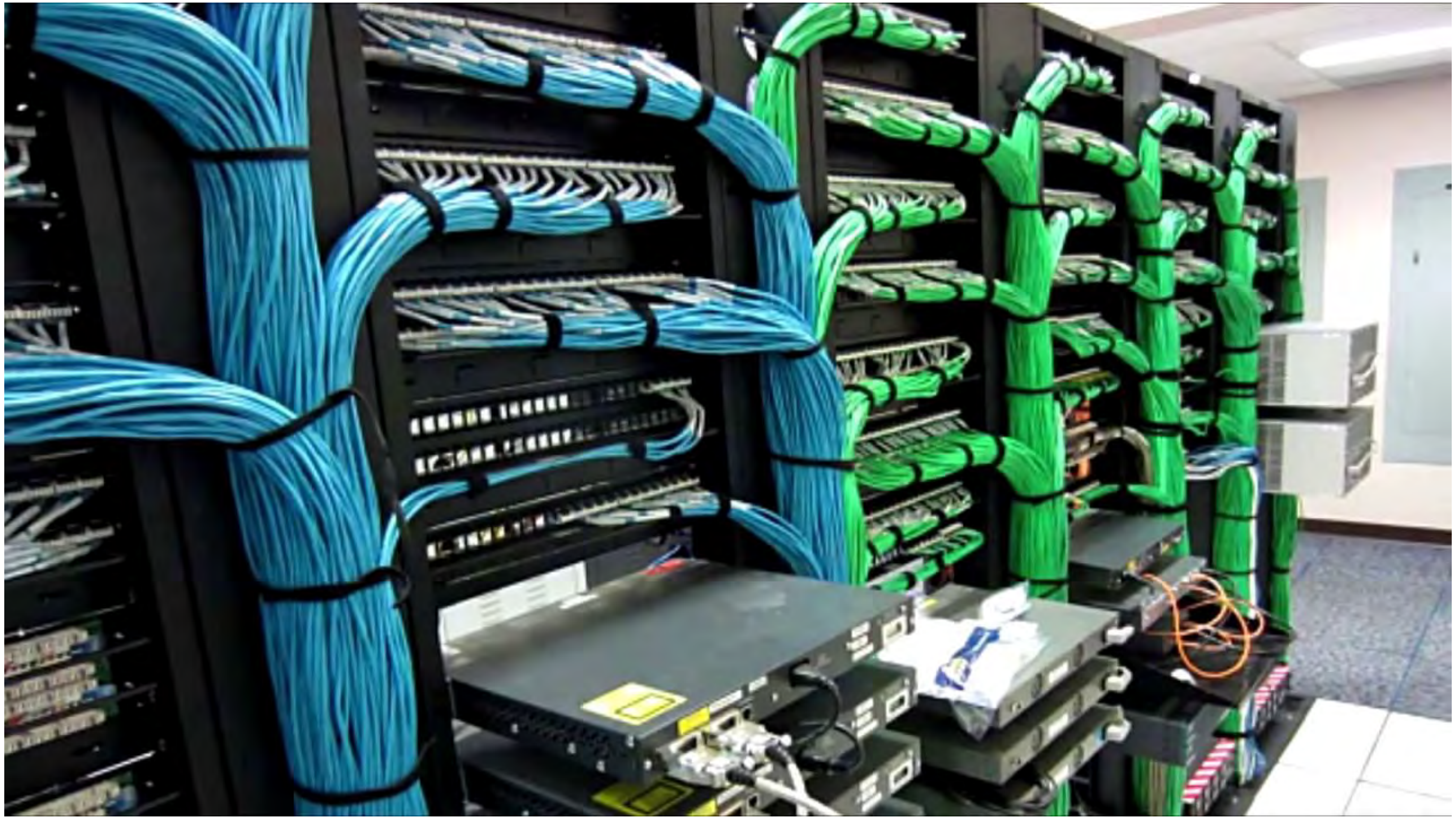
Good Cable Management



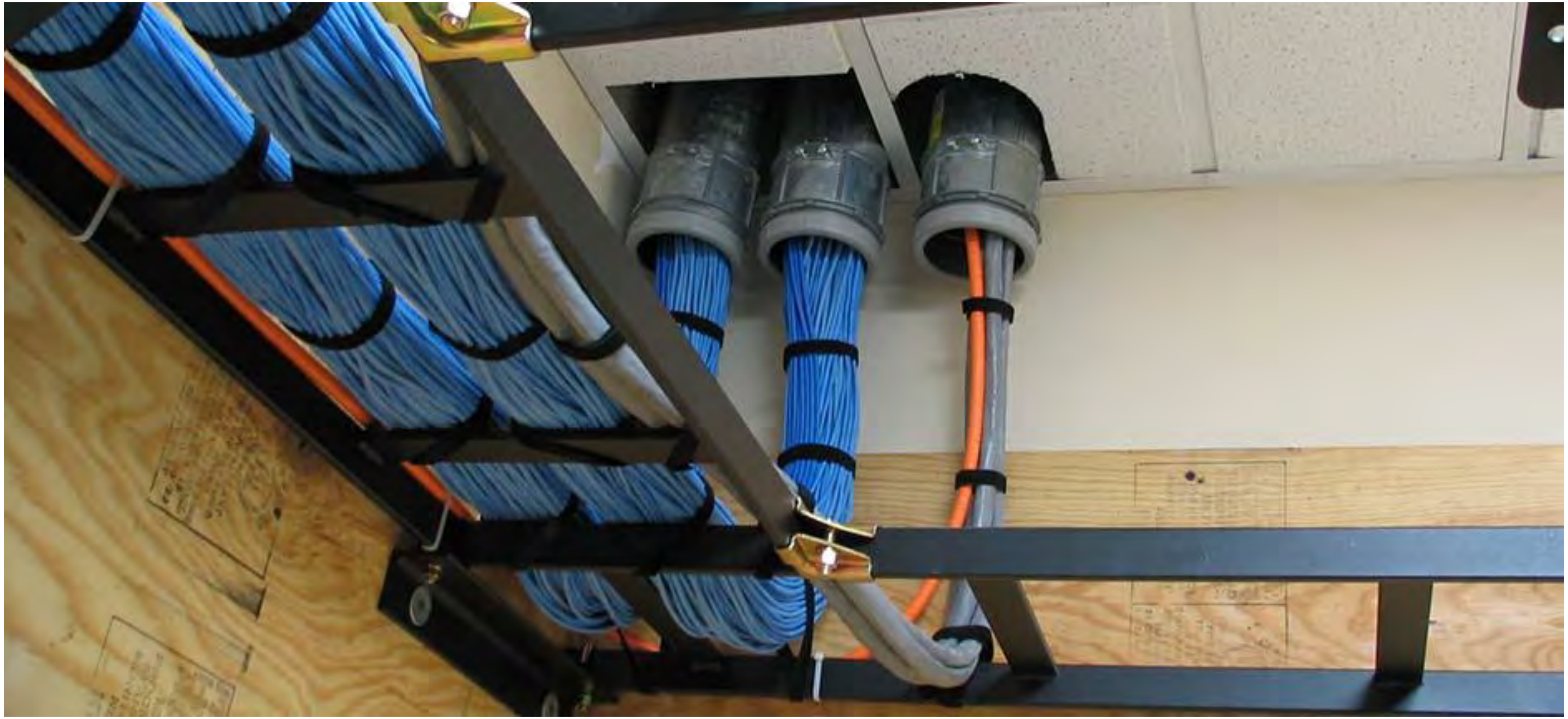
Good Cable Management (cont’d)



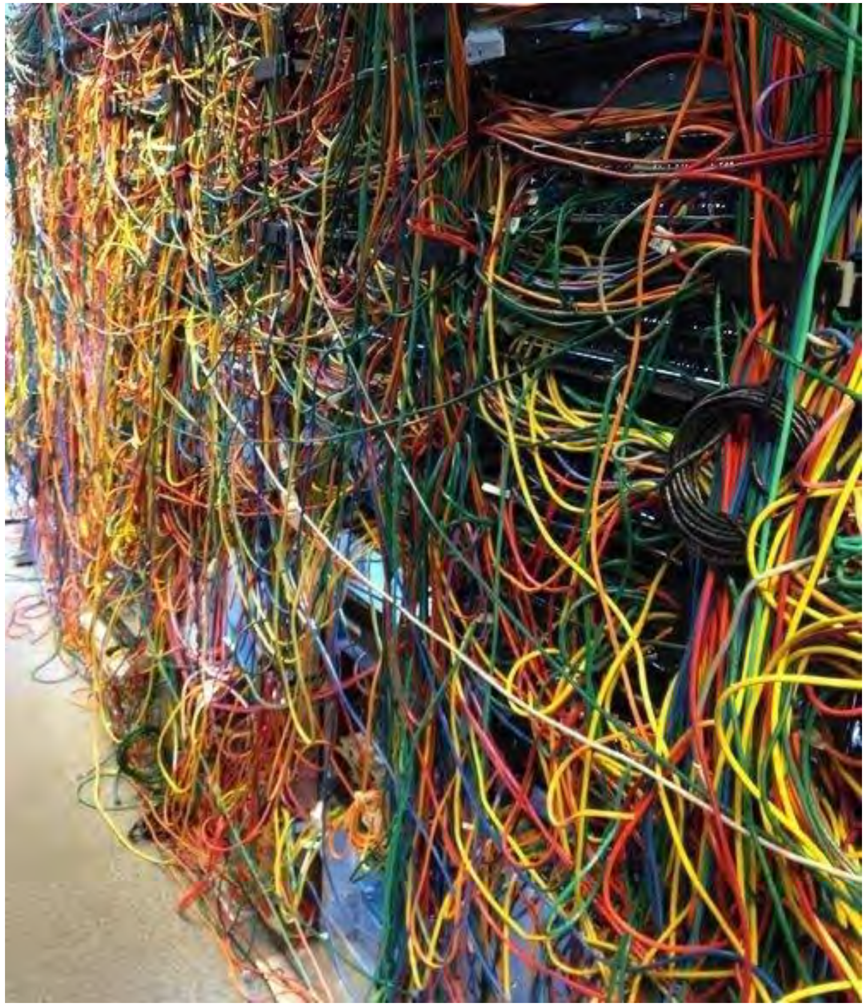
Good Cable Management (cont’d)

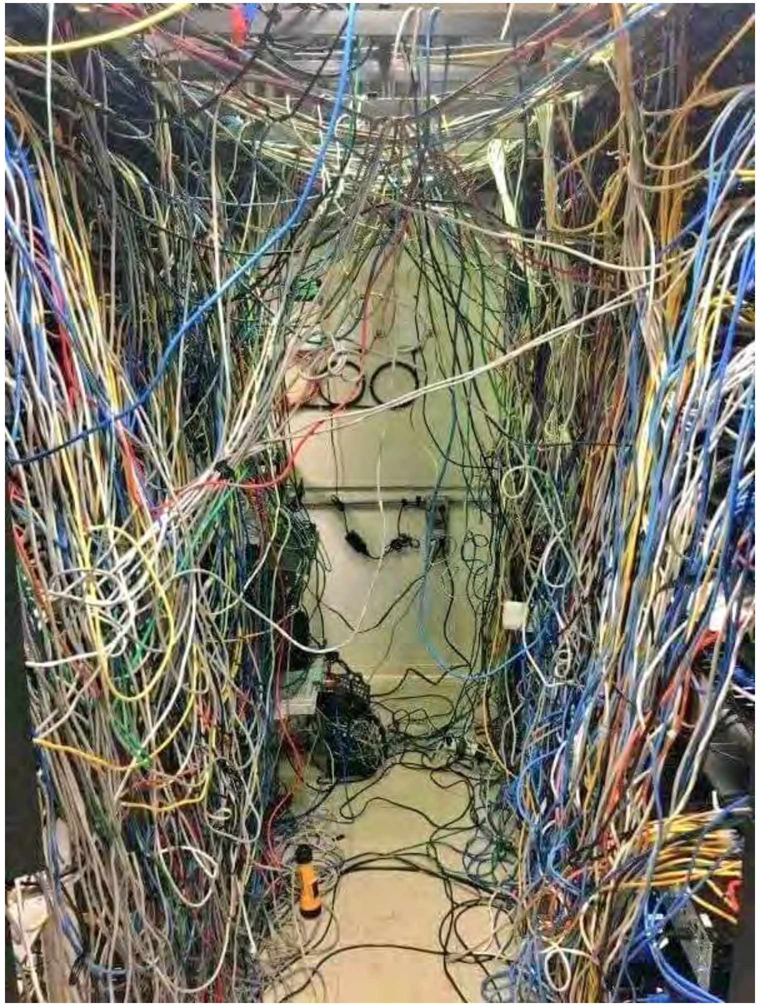


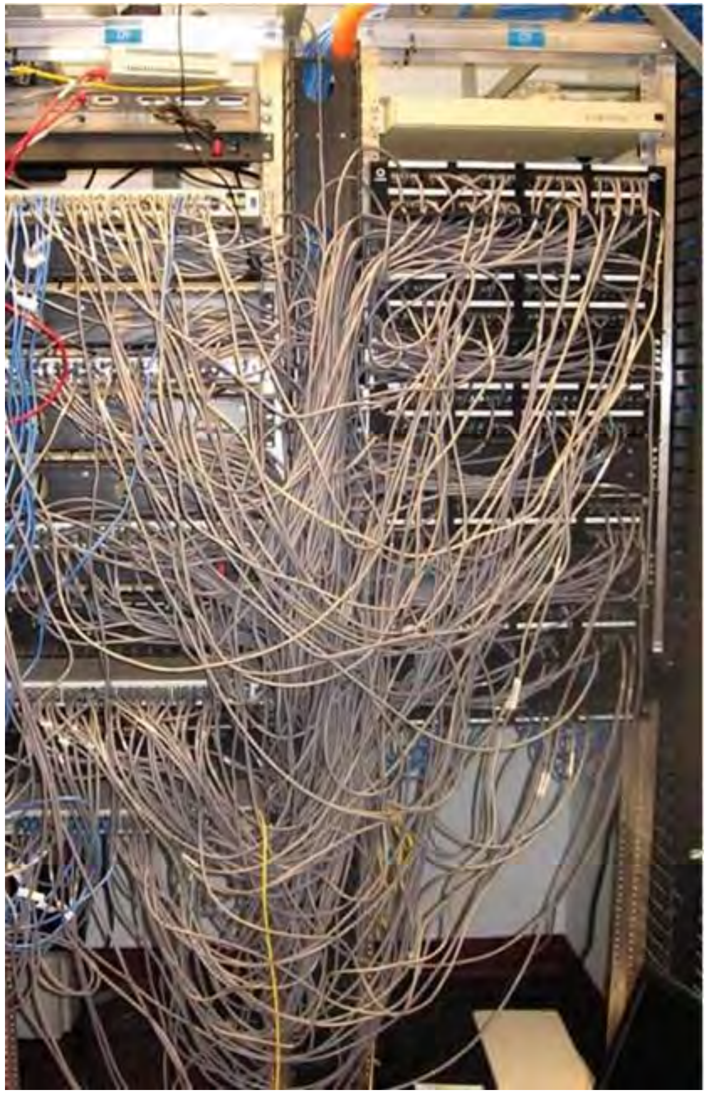
Good Cable Management (cont'd)



Don’t Do This!







Labeling

Why Label?

Easy identification of all devices and cabling

Numbering should follow a scheme that can be easily interpreted

Correlates to documentation

Facilitates initial installation, maintenance, and troubleshooting of devices, cabling, and data flow

Labeling Best Practices

Logical and consistent, across all locations, matching the project drawings

Identify the associated physical locations (building, room, cabinet, rack, port, etc.)

Easily read, durable, and capable of surviving for the life of the component that was labeled

The labeling system, and the identifiers used, must be agreed upon by all stakeholders

Should be pervasive

You should label:

- Cables and connecting hardware
  - Both ends of a patch cable or raw cable run BEFORE you install it!
- Fire stops, grounding and bonding locations
- Racks, cabinets, ports, and telecommunications spaces
- Servers, network devices
- WAN links
- User information

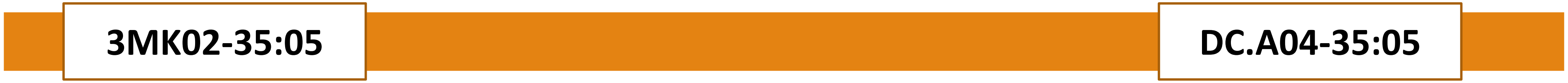
ANSI/TIA-606-B

A voluntary standard

Establishes the labeling and record keeping standards for:

- telecommunications and network systems
- industrial, residential, and healthcare facilities

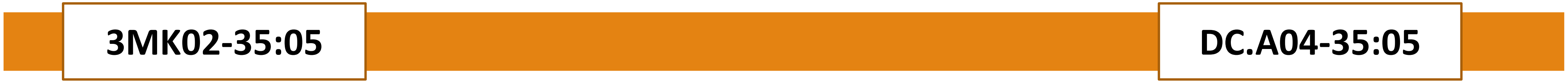
ANSI/TIA-606-B Example



3MK02-35:05/DC.A04-35:05

/ Separates the near end identification from the far end identification

ANSI/TIA-606-B Example



3MK02-35:05

DC.A04-35:05

3MK02 – The first element identifies the rack location at the near end of the cable.

- “3” = third floor
- “MK” = marketing department
- “02” = second cabinet in that third-floor marketing equipment room

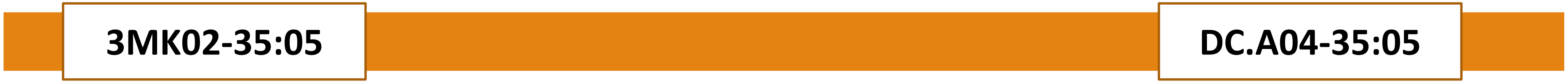
-35 = Patch panel located 35 rack units from bottom of cabinet

- specified as 3MK02 just previously

:05 = Specific port in the patch panel

- This is port 05.

ANSI/TIA-606-B Example



3MK02-35:05

DC.A04-35:05

DC.A04 = Cabinet location, but this time for the far end of the cable

- Far end of the cable is in the Data Center (DC)
- Fourth cabinet in row “A.”

-35 = The patch panel located 35 rack units from the bottom of the cabinet in question, A04

:05 = Specific port in the patch panel

Surveys and Assessments

Site Survey

Physical visit and walkthrough of an existing or potential location

- Used to identify existing or potential challenges to installing or upgrading the network

Produces an actionable, multi-level report with executive summary as well as annotated floor plans and technical details

Survey notes should be superimposed over a floor plan

Should include:

- Dimensions/distances
- Obstructions
- Recommended cabling paths and equipment placement
- Existing/supporting infrastructure
- Inter-floor/inter-building pathways or potential pathways
- Electrical outlets and power sources
- Environmental conditions
- Anything else that might impact installation or operation of the network

Might include a checklist of tasks that must be performed by the electrician, general contractor, client, etc. before the installation can begin

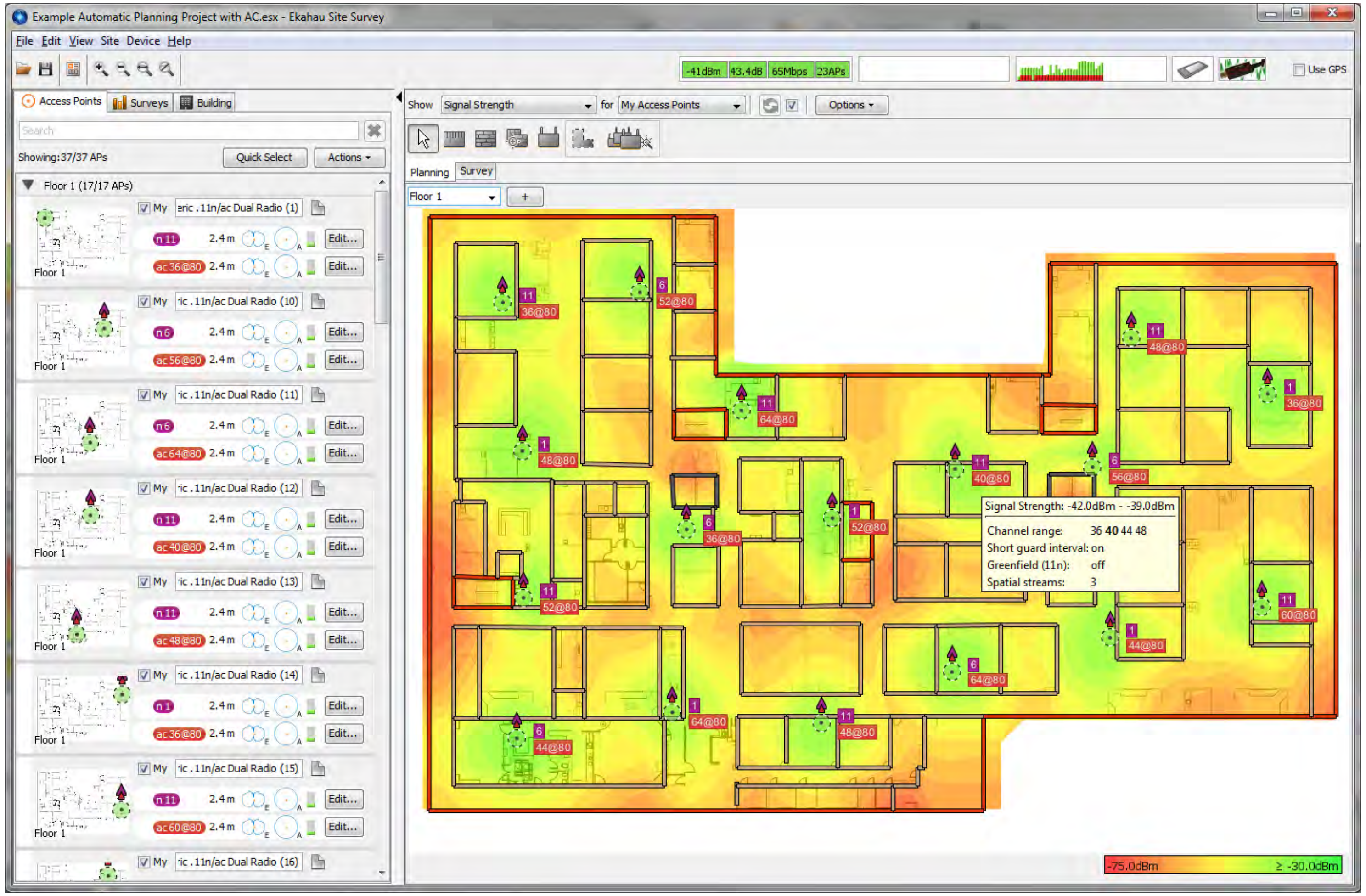
Wireless Site Survey

Many site surveys are conducted to add wireless to the LAN

A wireless site survey focuses on:

- Required coverage
- Antenna placement and design
- Cable distances
- Power distribution to access points
- Placement of wireless controllers
- Physical obstructions to RF signal
- Potential RFI/EMI interference sources

Wi-Fi Coverage Heat Map Example



Example Automatic Planning Project with AC.esx - Ekahau Site Survey

File Edit View Site Device Help

-41dBm 43.4dB 65Mbps 23APs

□ Use GPS

Access Points | Surveys | Building

Showing:37/37 APs

Quick Select | Actions ▾

Floor 1 (17/17 APs)

☑ My	eric .11n/ac Dual Radio (1)		
n 11	2.4 m	Edit...	Floor 1
ac 36@80	2.4 m	Edit...	
☑ My	ic .11n/ac Dual Radio (10)		
n 6	2.4 m	Edit...	Floor 1
ac 56@80	2.4 m	Edit...	
☑ My	ic .11n/ac Dual Radio (11)		
n 6	2.4 m	Edit...	Floor 1
ac 64@80	2.4 m	Edit...	
☑ My	ic .11n/ac Dual Radio (12)		
n 11	2.4 m	Edit...	Floor 1
ac 40@80	2.4 m	Edit...	
☑ My	ic .11n/ac Dual Radio (13)		
n 11	2.4 m	Edit...	Floor 1
ac 48@80	2.4 m	Edit...	
☑ My	ic .11n/ac Dual Radio (14)		
n 1	2.4 m	Edit...	Floor 1
ac 36@80	2.4 m	Edit...	
☑ My	ic .11n/ac Dual Radio (15)		
n 11	2.4 m	Edit...	Floor 1
ac 60@80	2.4 m	Edit...	
☑ My	ic .11n/ac Dual Radio (16)		

Show: Signal Strength for: My Access Points ☑ Options ▾

Planning | Survey

Floor 1 ▾ +

Signal Strength: -42.0dBm - -39.0dBm

Channel range: 36 **40** 44 48
Short guard interval: on
Greenfield (11n): off
Spatial streams: 3

-75.0dBm ≥ -30.0dBm

Predictive Site Survey

A virtual site survey

Uses relevant information about the site to plan the network installation or upgrade

Saves money over the traditional survey

Commonly used in consumer installations

Makes assumptions and may miss actual physical issues

Should only be used if:

- You are already intimately familiar with the site
- You price the quote high, to include all possible contingencies

Audit and Assessment Report

You should regularly conduct a security audit to identify potential risks

The audit should include:

- Network and device vulnerability scan
- Policy assessment (does it need to be updated)
- Training effectiveness
- Risks to facilities, people and processes
- Penetration testing (optional but strongly recommended)
- Overall security posture

Preferably, the audit should be conducted by a certified, neutral third party

The audit should produce an actionable report with

- Executive summary
- Technical details
- Recommended remediation steps
- Recommended or required remediation timelines