



HARVARD EXTENSION SCHOOL

CSCI E-117A SPRING 2025

SECURE APPLICATIONS: MANAGING THE DEPLOYMENT
INFRASTRUCTURE

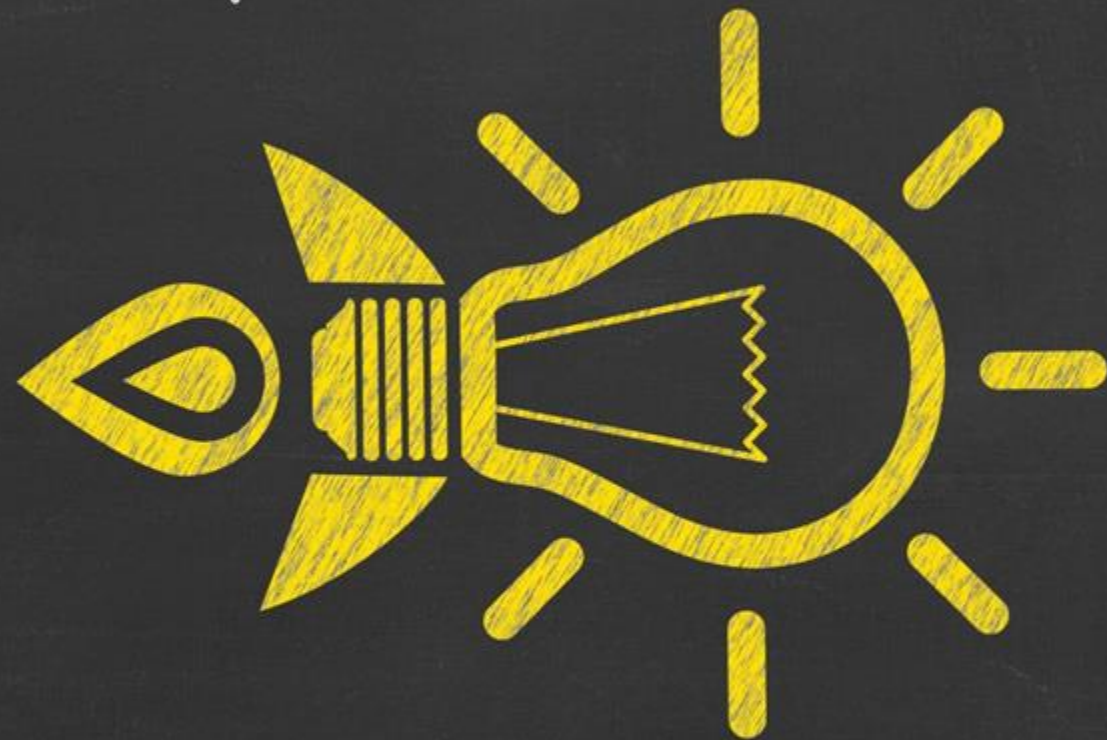
Lecture 3
Feb 11, 2025

LECTURE 3 & 4

AGENDA

- YellowDig last week
- Course Assignment reminders
- Networks
 - Network Architectures
 - Network Stack Intro
 - Stack-level threats
- Network Protocol Vulnerabilities
- Network Zero Trust Architecture
- Industrial Control Systems (ICS) and ZTA
- Vulnerabilities
 - Known Exploitable

YELLOW DIG LAST
WEEK



LINUX KNOWN EXPLOITABLE VULNERABILITY CVE-2024-53104

<https://www.cisa.gov/news-events/alerts/2025/02/05/cisa-adds-one-known-exploited-vulnerability-catalog>

https://www.theregister.com/2025/02/04/google_android_patch_netgear/

ALERT

CISA Adds One Known Exploited Vulnerability to Catalog

Release Date: February 05, 2025



CISA has added one new vulnerability to its [Known Exploited Vulnerabilities Catalog](#), based on evidence of active exploitation.

■ [CVE-2024-53104](#)  Linux Kernel Out-of-Bounds Write Vulnerability

These types of vulnerabilities are frequent attack vectors for malicious cyber actors and pose significant risks to the federal enterprise.

YELLOW DIG LAST WEEK

- This CVE was rated a 1.8 on the CVSS exploitability subscore. Why? Because it actually requires a chain of exploiting 4 other CVEs the Linux kernel published. This just happens to be one of the CVEs in the exploit chain.
- This vulnerability only applies to [kernel implementations in Android's version of Linux](#). The flaw doesn't apply to kernels in servers or other devices. At all... [YET] There's no mention of the other CVEs in the attack chain.
- Now, this is a really bad CVE. Exploiting this vulnerability allows anyone to plug a malicious USB-C device into an Android phone and have instant root access to the phone.
- Did you get all that context from reading the links? I didn't...

THE REGISTER, SC MEDIA THOUGHTS ON CVE-2024-53104

The Register

- The flaw, [CVE-2024-53104](#), is an intriguing [Linux kernel flaw](#) in its USB video-class driver code. There's not a lot of detail about the bug, other than the fix is to skip the parsing of undefined video frames that would otherwise cause the kernel to write to memory it's not supposed to, which could be used to crash or fully hijack a device.
- What's interesting is that this driver code is supposed to mainly handle USB cameras and similar video sources. Thus, exploitation potentially involves connecting some malicious hardware that feeds bad data into the system. Google indicated the flaw can be used to achieve "physical escalation of privilege with no additional execution privileges needed," which to us sounds like someone being able to plug a malicious gadget – perhaps something law enforcement might use – into a vulnerable Android device and taking it over. Very curious.
- Of the [46 patches](#) pushed out by Google this month, only one is rated as "critical" by the ad slinger: CVE-2024-45569, with a CVSS rating of 9.8 out of 10.

SC Media

- CISA's order follows Google issuing a patch for the bug — [CVE-2024-53104](#) — mainly because the flaw could let attackers escalate privileges on the Linux operating systems that run many of its popular [Android](#) and Google Pixel devices.

Vulnerability Name	Date Added	Due Date	Required Action
Linux Kernel Out-of-Bounds Write Vulnerability	02/05/2025	02/26/2025	Apply mitigations per vendor instructions or discontinue use of the product if mitigations are unavailable.

Known Affected Software Configurations [Switch to CPE 2.2](#)

Configuration 1 ([hide](#))

🔗 cpe:2.3:o:linux:linux_kernel:*:*:*:*:*:* Show Matching CPE(s) ▼	From (including) 2.6.26	Up to (excluding) 4.19.324
🔗 cpe:2.3:o:linux:linux_kernel:*:*:*:*:*:* Show Matching CPE(s) ▼	From (including) 4.20	Up to (excluding) 5.4.286
🔗 cpe:2.3:o:linux:linux_kernel:*:*:*:*:*:* Show Matching CPE(s) ▼	From (including) 5.5	Up to (excluding) 5.10.230
🔗 cpe:2.3:o:linux:linux_kernel:*:*:*:*:*:* Show Matching CPE(s) ▼	From (including) 5.11	Up to (excluding) 5.15.172
🔗 cpe:2.3:o:linux:linux_kernel:*:*:*:*:*:* Show Matching CPE(s) ▼	From (including) 5.16	Up to (excluding) 6.1.117
🔗 cpe:2.3:o:linux:linux_kernel:*:*:*:*:*:* Show Matching CPE(s) ▼	From (including) 6.2	Up to (excluding) 6.6.61
🔗 cpe:2.3:o:linux:linux_kernel:*:*:*:*:*:* Show Matching CPE(s) ▼	From (including) 6.7	Up to (excluding) 6.11.8
🔗 cpe:2.3:o:linux:linux_kernel:*:*:*:*:*:* Show Matching CPE(s) ▼	From (including) 6.12	Up to (excluding) 6.12.1

- <https://nvd.nist.gov/vuln/detail/CVE-2024-53104>
- REMINDER: This CVE was rated a 1.8 [since upgraded to 7.8] on the CVSS exploitability subscore. Why? Because it actually requires a chain of exploiting 4 other CVEs the Linux kernel published. This just happens to be one of the CVEs in the exploit chain.
- CISA says: its on KEV, patch immediately
- CVE.org lists impacted/not impacted O/S
- NVD says: patch or take offline
- DISCUSS (Take a position either way and justify):
 - CISA {SHOULD, SHOULD NOT} disclose the full set of vulnerabilities in the attack chain to the public. Why.

CLASS DISCUSSION: HOW MUCH SHOULD BE DISCLOSED



- *END OF CLASS*
- *This is never an “old” conversation – its another one of those “it depends” conversations*
- *How much SHOULD be disclosed about the Linux vulnerability?*

DISCUSSION LAST WEEK

- *From the Poll, Class Discussion and Canvas Discussion, this point was raised and is important enough that it is highlighted here*
- *Is this type of information more or less meaningful to you than information about the environment (production v dev/test)?*
 - No, the data being stored does not make much of a difference whether it be DEV, QA, STAGE, TEST, PROD etc.
 - Typically, Dev will use fake data that reflects customer data

YELLOWDIG LAST WEEK

- Boards tend to rely on a cyber security program to achieve a level of maturity but often fail, or are challenged, to understand that the threat landscape is a moving target and that innovation, evolution is necessary.
- ... I think the comment about Boards not understanding the complex landscape is not necessarily fair! When I took the Cybersecurity and the Law class with Professors Cass and Garrie, we discussed having cyber experts on boards. While this may not be the norm today, I think in the next 5 years we could start seeing more cyber experts being represented, at least for large corporations because of the evolving nature of cyber threats.

YELLOWDIG LAST WEEK

- Our legacy models of security were designed for a world that no longer exists. The interconnectedness of today's digital environment has outpaced the foundational assumptions we once relied upon, and this disconnect has left us vulnerable to ever-evolving threats like ransomware
- The military taught me that trust must be proportional to transparency and accountability. We cannot simply trust that the systems we've built are secure; we must continuously validate and question them.
- Yet many startups, in their rush to scale, overlook the importance of secure-by-design principles, leaving their systems vulnerable. The lesson here is clear: we must build security into every layer of our systems and question whether our solutions are truly equipped to handle modern threats. Incremental improvements will not suffice; we need bold changes and significant investments
- Cybersecurity is not just a technical problem; it's a human one. The "human factor" remains one of the greatest vulnerabilities in any system.

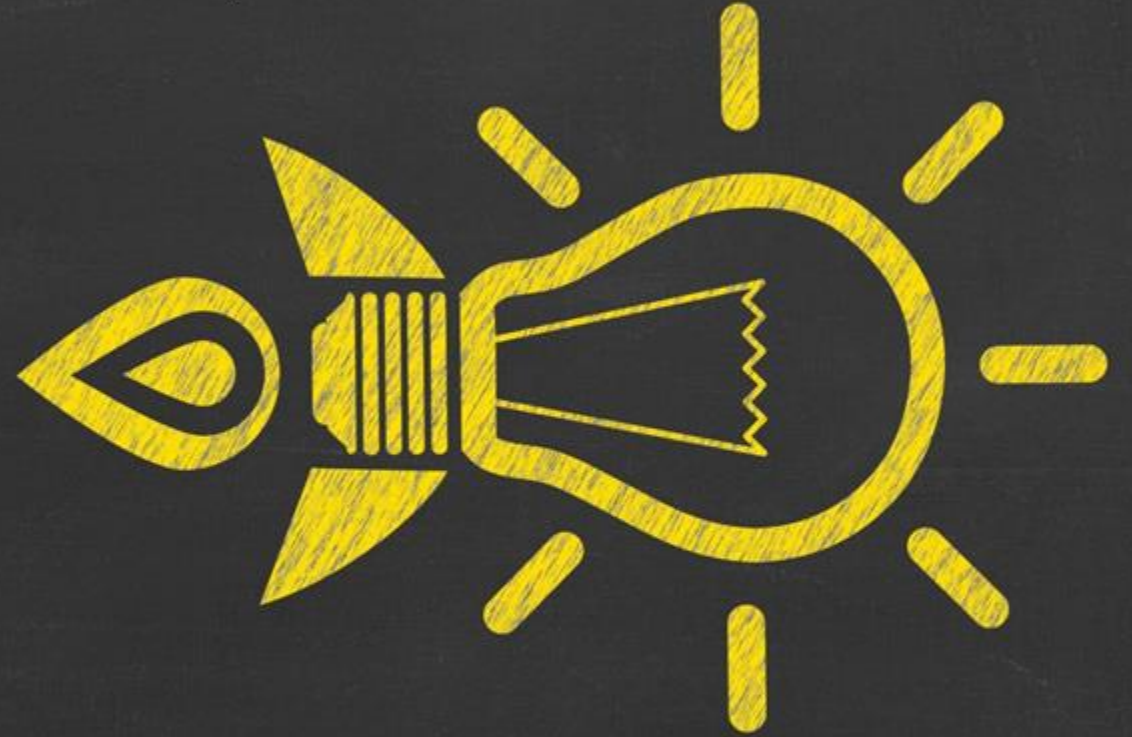
YELLOWDIG LAST WEEK

- ...back in 80s - there was the theory of developing systems demonstrably secure in the form of mathematical proofs - but we never went down that path. So baseline system integrity is assumed, and we are operating on that - the idea of eliminating entire classes of attacks is too daunting ".
- My view is that rather than relying on security products or a security platform such as mimic that try to detect and respond to threats using MTD or other means, we should focus on designing secure systems from the ground up, with mathematical proofs backing their execution.
- Faster does not equate to smarter or better security - it is yet another smoke screen - false sense of security.



YELLOWDIG LAST WEEK

ASSIGNMENTS



ASSIGNMENT 1



Due Date: Feb 16

Purpose: Start to think about threats to the network, device and application asset classes, and as a bonus, the impact of GenAI in the attack and defense of the asset classes.

Assignment 1 Details

Sample answer for
"MyFuBar" Asset class

Question 1A (10 points)				
Asset Class	Priority #1	Priority #2	Priority #4	
<i>MyFuBar Asset Class</i>	<i>Integrity</i>	<i>Availability</i>	<i>Confidentiality</i>	
Network	Pick One: Confidentiality, Integrity, Availability	Pick One: Confidentiality, Integrity, Availability	Pick One: Confidentiality, Integrity, Availability	
Device	Pick One: Confidentiality, Integrity, Availability	Pick One: Confidentiality, Integrity, Availability	Pick One: Confidentiality, Integrity, Availability	
Application	Pick One: Confidentiality, Integrity, Availability	Pick One: Confidentiality, Integrity, Availability	Pick One: Confidentiality, Integrity, Availability	
Ordering, meet rules of assignment				

3 marks, 1 per cell

3 marks, 1 per cell

3 marks, 1 per cell

(Additional) 1 mark

Assignment 1 Details

Question 1B (15 points, 5 per asset class)	Your Answer
Networks: Control Order Justification:	<i>Answer here</i>
Devices: Control Order Justification:	<i>Answer here</i>
Applications: Control Order Justification: Your an	<i>Answer here</i>
If you used Generative AI to help with your answers, you MUST include the prompt that you used.	<i>Prompt used:</i>

ASSIGNMENT 2



Due Date: Mar 2

Purpose: To look at the network asset class in more detail, from a zero trust point of view, a threat point of view and a protection point of view.

Started: Feb 11 at 3:29pm

Quiz Instructions

For the purposes of this assignment, we are considering the Course Discussion Environment hosting VARY. In this assignment, you have different areas / functions of your environment that you must pay attention to:

- Your (cloud hosted) development environment, including your build pipeline
- Your (cloud hosted) test environment, where you test new functionality
- Your (cloud hosted) Blue/Green production environments made up of a Blue environment and a Green environment
 - To start with, Blue and Green are identical, Green is marked as Production and Blue is marked as Change/Patch/Backup
 - Changes are tested in Blue, including patches, major function updates and so on. If and when your green environment is not available / is compromised or when you have to roll out major changes that include disruptive patches and updates, that have been tested and proved in Blue, you will roll production over from Green to Blue, treat Blue as production, apply all those disruptive updates to Green and use Green for change testing, patches, etc until you are ready to flip flop back from Blue to Green.
- Your co-lo hosted backup/storage environment

[CSC117-Spring2025-Assign2.docx](#) ↓ (opens as document file)

Question 1: Given the environment description above, map the best "fitting" MITRE ATT&CK technique to the Zero Trust Architecture network class. By "fit" we mean the MITRE ATT&CK technique that is the most effectively addressed / remediated / mitigated by the ZTA network class.

So pick the technique that is prevented or severely limited by

- Network Segmentation
- Network Traffic Monitoring
- Traffic Encryption
- Network Resilience

For this question there are right and wrong answers.

Network Segmentation	<div>[Choose]</div>	
Network Traffic Management	<div>[Choose]</div>	<div>Network Segmentation</div>
Traffic Encryption	<div>[Choose]</div>	<div>Network Traffic Management</div>
Network Resilience	<div>[Choose]</div>	<div>Traffic Encryption</div>

✓ [Choose]

Browser Session Hijacking - MITRE TECHNIQUE REFERENCE: <https://attack.mitre.org/techniques/T1185/>
Brute Force - MITRE TECHNIQUE REFERENCE: <https://attack.mitre.org/techniques/T1110/>
Active Scanning / IP Blocks - MITRE TECHNIQUE REFERENCE: <https://attack.mitre.org/techniques/T1595/001/>
Compromise Infrastructure: Botnet - MITRE TECHNIQUE REFERENCE: <https://attack.mitre.org/techniques/T1584/005/>
Network Boundary Bridging - MITRE TECHNIQUE REFERENCE: <https://attack.mitre.org/techniques/T1599/>
Adversary-in-the-Middle - MITRE TECHNIQUE REFERENCE: <https://attack.mitre.org/techniques/T1557/>

Question 2A:

Zero Trust Network Architecture prioritization ("fill in the blanks")

Network segmentation is

1 1

Network Traffic Management is

2 1

Traffic Encryption is

3 3

Network Resilience is

4

For this question, the ordering is selected by you, you have the option to pick the ordering. Even though the quiz selection in theory would allow you to pick all four as priority 2 (for example), or pick one as priority 1, two as priority 2 and one as priority 4. THIS IS NOT ALLOWED PER THE RUBRIC.

You must rank only one as priority 1 (the highest priority), only 1 as priority 2, only 1 as priority 3, and only 1 as priority 4. You will get a 0 for each ranking that is a duplicate or re-use of another ranking.

Question 2B

In 2-3 sentences, justify which ZTA Network class you selected as priority #1.

Your justification should mention / include threats, likelihood of compromise due to unprotected/poorly protected network architecture, severity of compromise, intrusiveness & cost of the program to implement the network architecture controls in terms of dollars, people, time.

Edit View Insert Format Tools Table

12pt ▾ Paragraph ▾ | **B** *I* U A ▾  ▾ T^2 ▾ | ⋮

Question 7

1 pts

Of the CISO network control categories, which ONE (pick one only) do you think is the most likely to benefit from Generative AI based DEFEND capabilities

• Network Segmentation

• Network Traffic Management

• Traffic Encryption

• Network Resilience

Fill in the blanks
with a “X” or “ “
“X” means you think
it is the one that is
most likely to
benefit

ASSIGNMENT 3



Due Date: Mar 9

To be released no later than Feb 23

Purpose: To look at the device asset class in more detail, from a zero-trust point of view, a threat point of view and a protection point of view.

ASSIGNMENT 4



Due Date: Mar 30

To be released no later than Mar 2

Purpose: To look at the (TBD applications, data, identity) asset class in more detail, from a zero trust point of view, a threat point of view and a protection point of view.

CAPSTONE ASSIGNMENT

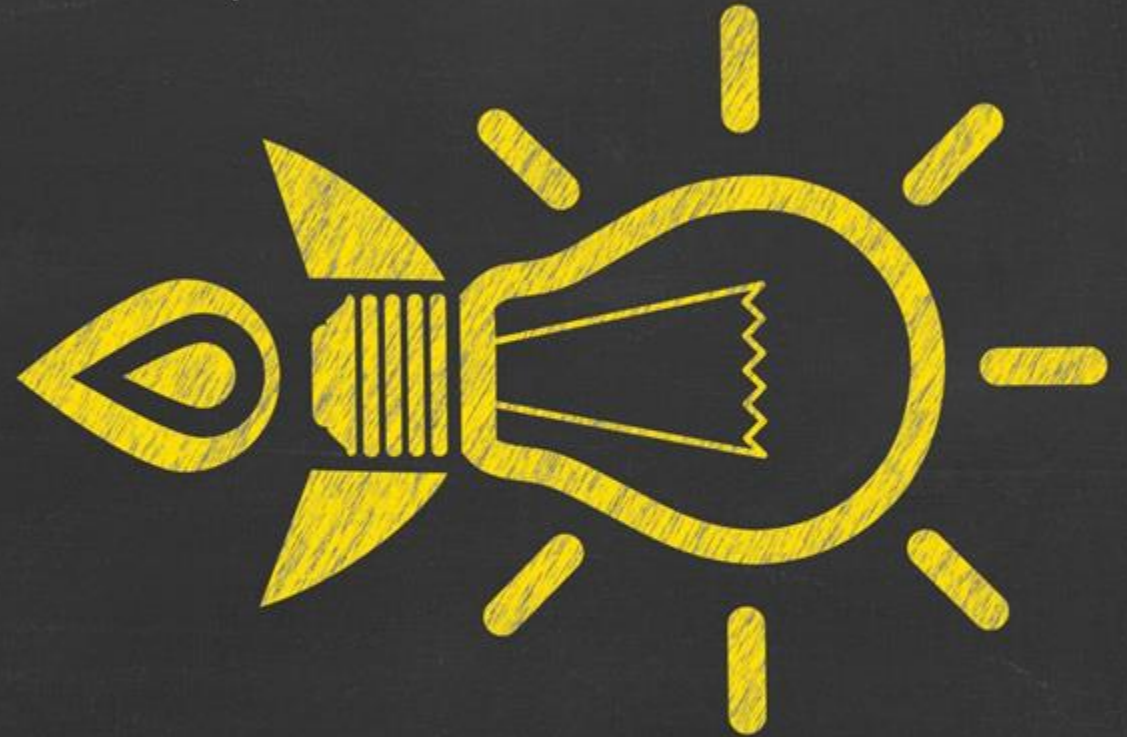


Due Date: SATURDAY MAY 3

To be released no later than March 31

Purpose: To reflect on the intersection and benefits of a zero trust versus a secure by design versus a threat and risk point of view, given that "you can't have it all, but still have to protect an environment".



REMINDERS



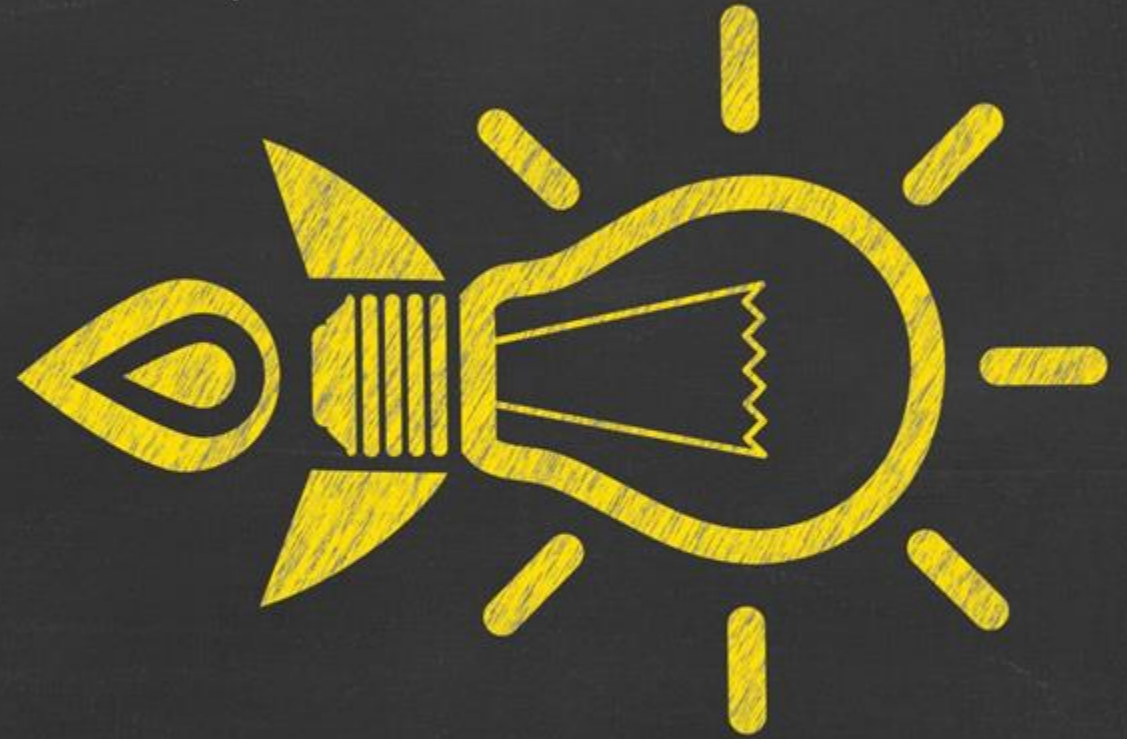
Asset Class	Examples
Network	<p>Communication channels, connections and protocols that enable traffic to flow among devices and applications.</p> <p>Note that this does NOT refer to the actual infrastructure (routers, switches) but rather to the paths themselves and the protocols used in those paths. This class includes VPC, VPN, CDN as well as DNS, BGP, email and web filtering, SSL/TLS, HTML</p>
Devices	<p>Workstations, servers, phones, tablets, IoT, containers, hosts, compute, peripherals storage devices, network devices, web cameras, infrastructure, etc.</p> <p>This asset class includes the operating systems and firms of these devices as well as other software that is native to or inherent to the device. Networking devices like switches and routers are included here because the devices themselves need to be considered separately from the communication path they create.</p>
Applications	<p>Software code and applications on the devices, separate from the operating system/firmware. This class includes serverless functions, APIs and microservices.</p> <p>This also includes the business applications that support a company - from HR Systems (eg Workday), to Customer Relationship Management (eg Salesforce), to payroll, billing, and the applications that are “used” to do work (email,G Suite/Box, web conferencing, telephone systems)</p>
Data	<p>The information residing on (data-at-rest), traveling through (data-in-motion), or processed (data-in-use) the resources listed above.</p> <p>This class includes databases, S3 buckets, storage blobs, and files</p>
Users	<p>The people using the resources listed above and their associated identities.</p> <p>This includes customers (using the applications/services your company provides) and the employees of your company</p>

Zero Trust Architecture: Networks

A network refers to an open communications medium including typical channels such as agency internal networks, wireless networks, and the Internet as well as other potential channels such as cellular and application-level channels used to transport messages.

ZTA Focus	Network Segmentation	Network Traffic Management	Traffic Encryption	Network Resilience
Description	Segments / subnets with controlled access to move from flat to segmented network	Monitor traffic to track and analyse data flowing across a network; identify potential issues, understand usage patterns, and optimize performance	Point to point, End to end with robust key management 	System designed to withstand disruptions, recover quickly from failures, and maintain operational continuity even during unexpected events
Maturity Goal	Moving from perimeter-internal to “segments” that allow isolation of workloads in progressively more restrictive segments	Move from manual management of static rules and configurations to automation and dynamic rules and configurations including dynamically responding to new/emerging threats	Moving from minimal to comprehensive encryption of traffic including mutual authentication of parties as part of encryption	Move from limited resilience of networks to fully redundant and always available networks 

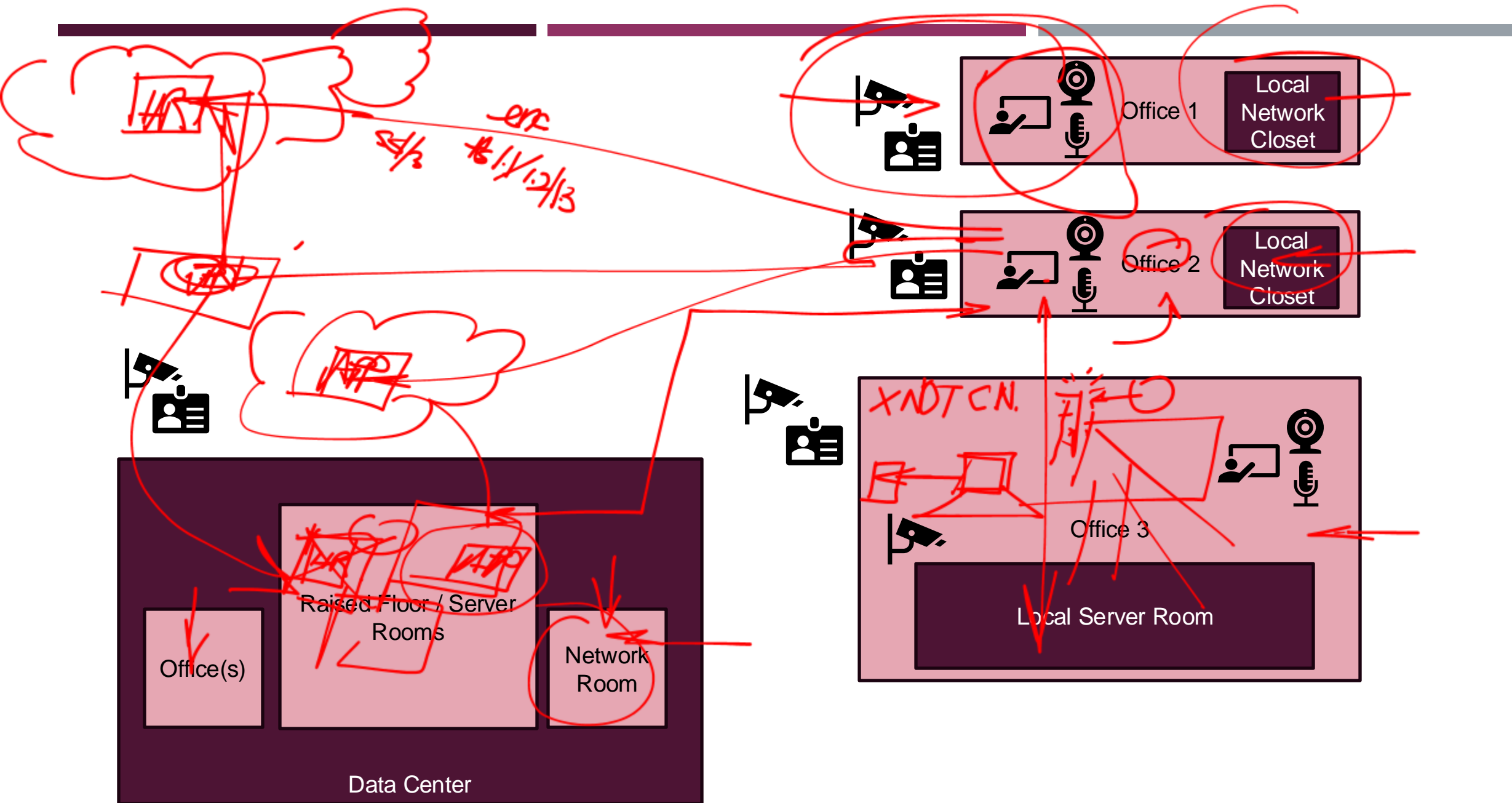
ZERO TRUST NETWORK ARCHITECTURE

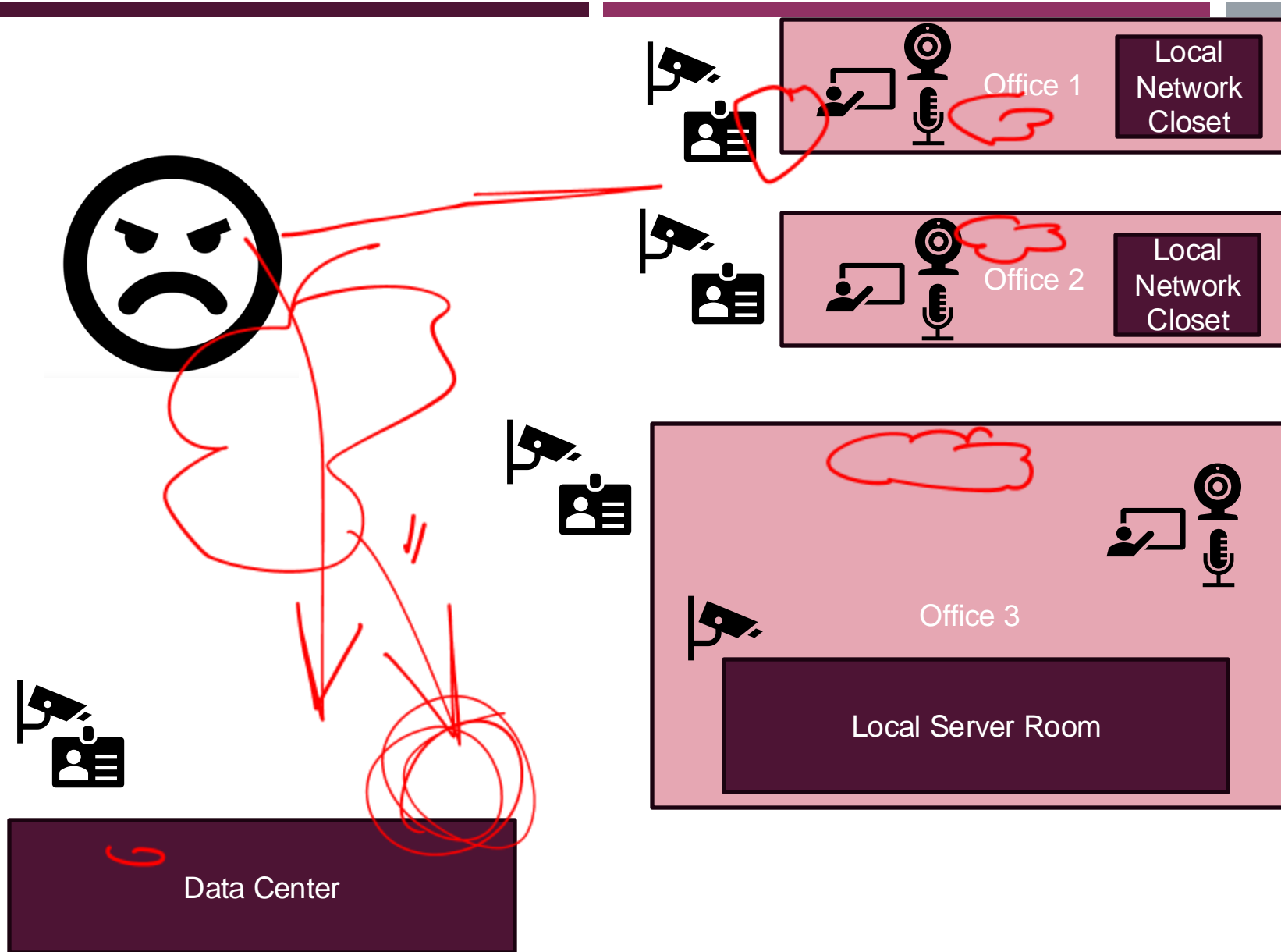


Zero Trust Architecture: Networks

A network refers to an open communications medium including typical channels such as agency internal networks, wireless networks, and the Internet as well as other potential channels such as cellular and application-level channels used to transport messages.

ZTA Focus	Network Segmentation	Network Traffic Management	Traffic Encryption	Network Resilience
Description	Segments / subnets with controlled access to move from flat to segmented network	Monitor traffic to track and analyse data flowing across a network; identify potential issues, understand usage patterns, and optimize performance	Point to point, End to end with robust key management	System designed to withstand disruptions, recover quickly from failures, and maintain operational continuity even during unexpected events
Maturity Goal	Moving from perimeter-internal to “segments” that allow isolation of workloads in progressively more restrictive segments	Move from manual management of static rules and configurations to automation and dynamic rules and configurations including dynamically responding to new/emerging threats	Moving from minimal to comprehensive encryption of traffic including mutual authentication of parties as part of encryption	Move from limited resilience of networks to fully redundant and always available networks



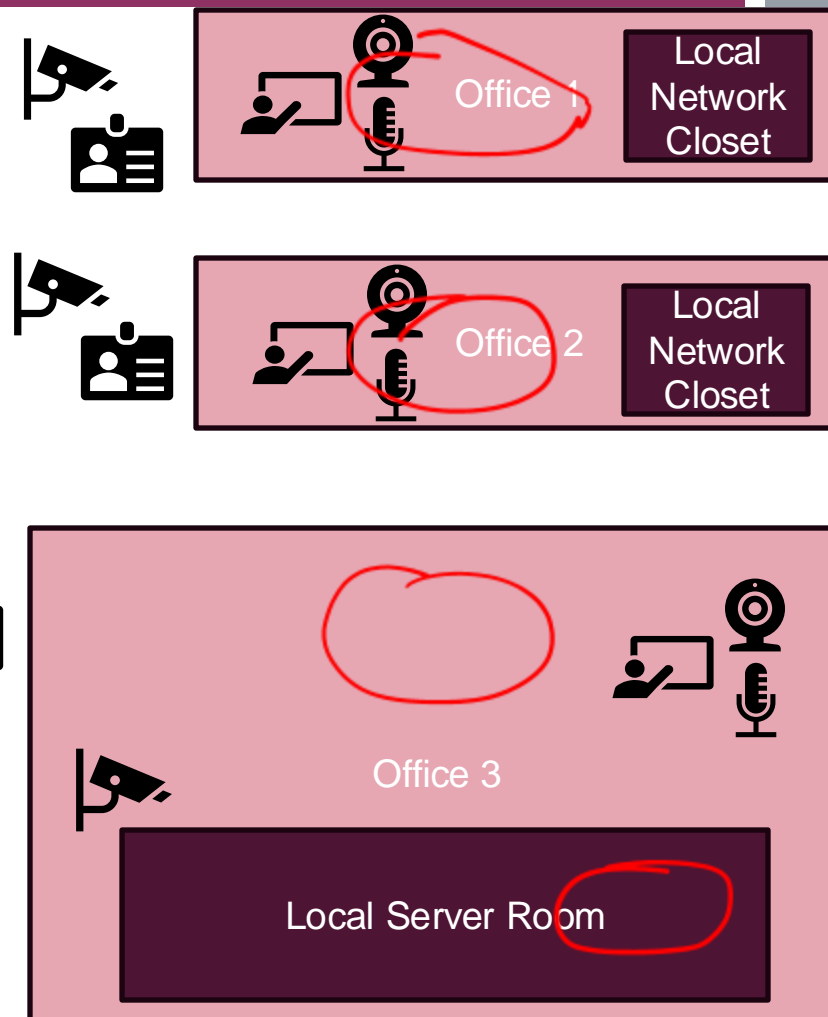
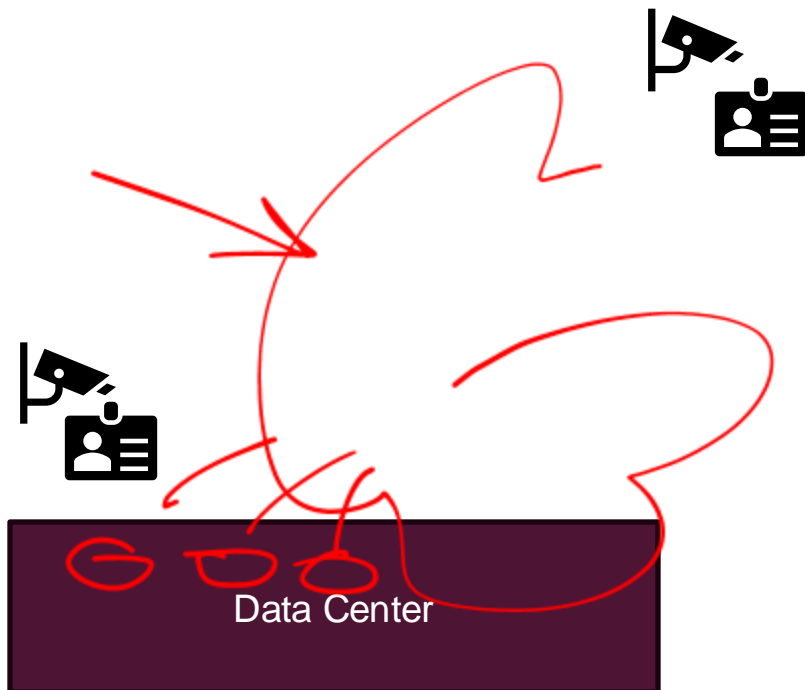


Network Protocols

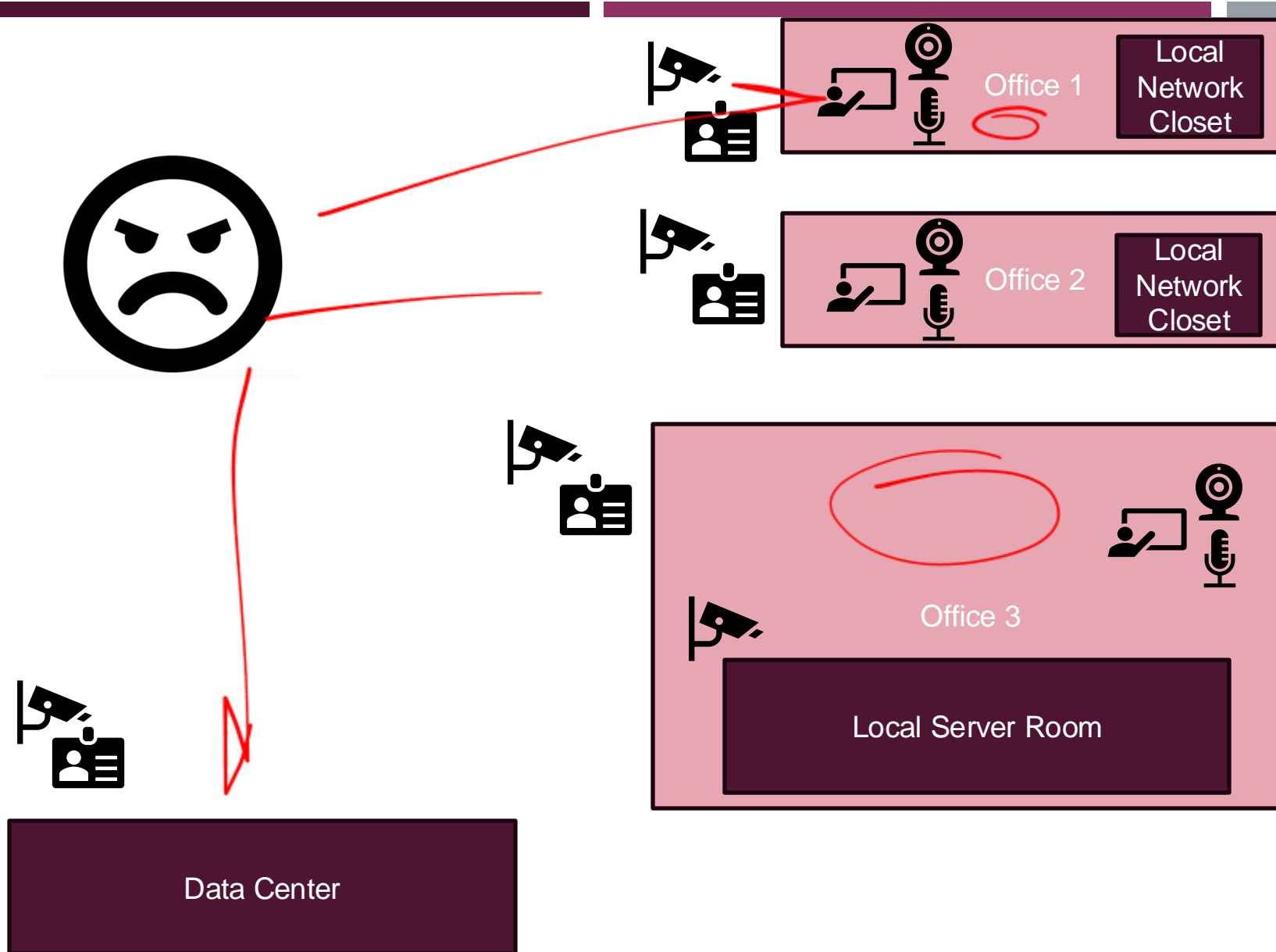
Enable traffic to flow among devices and applications.

TCP/IP Protocol Suite





Network Segmentation
Segments / subnets with <u>controlled access</u> to move from flat to segmented network



Network Traffic Management

Monitor traffic to track and analyse data flowing across a network; identify potential issues, understand usage patterns, and optimize performance

** Avail ->
* Perf*

Traffic Encryption

Point to point, End to end with robust key management

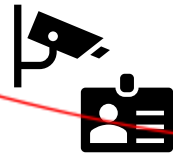


Data Center



Office 3

Local Server Room



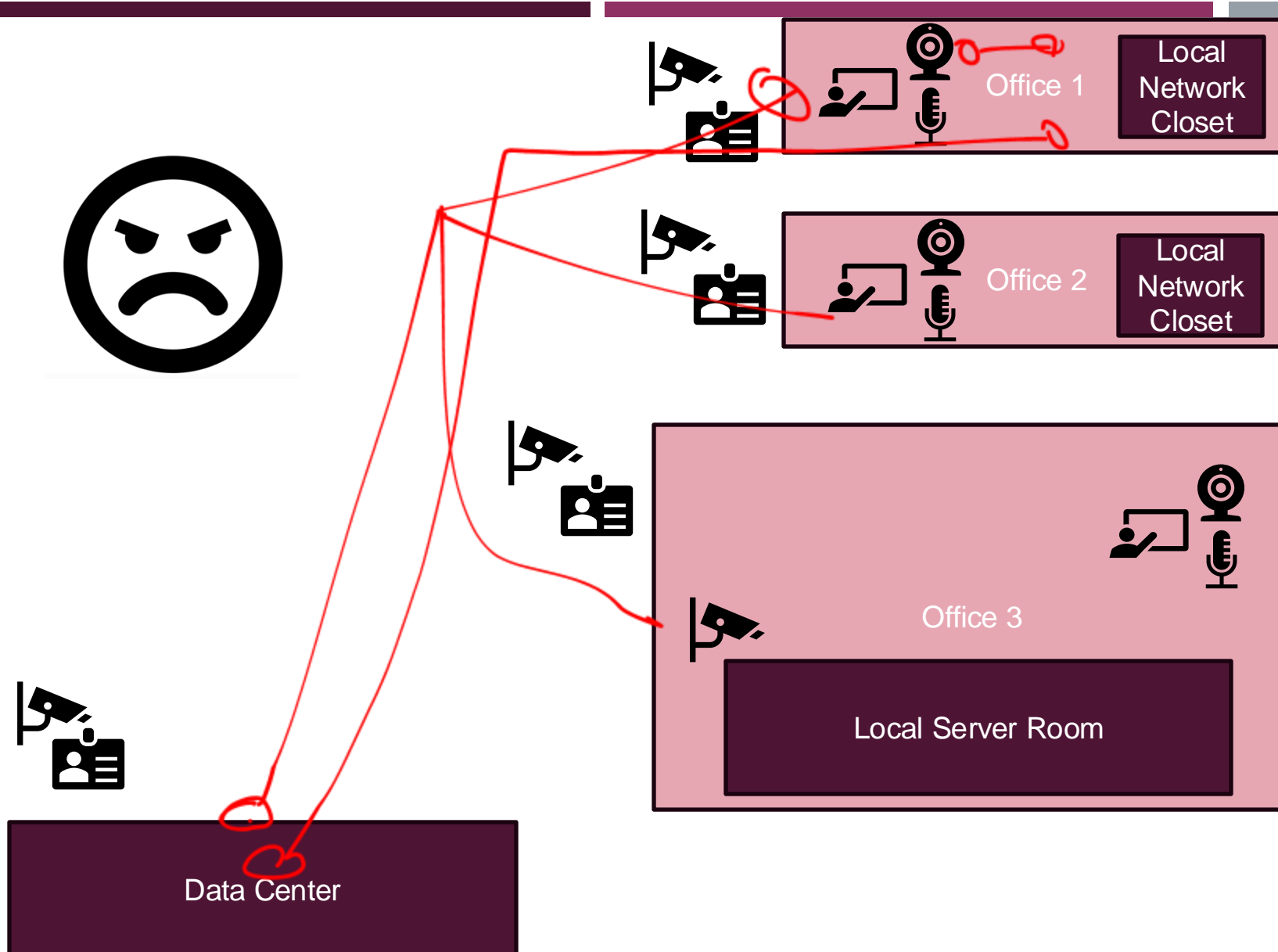
Office 2

Local Network Closet



Office 1

Local Network Closet





Data Center



Office 1

Local
Network
Closet



Office 2

Local
Network
Closet



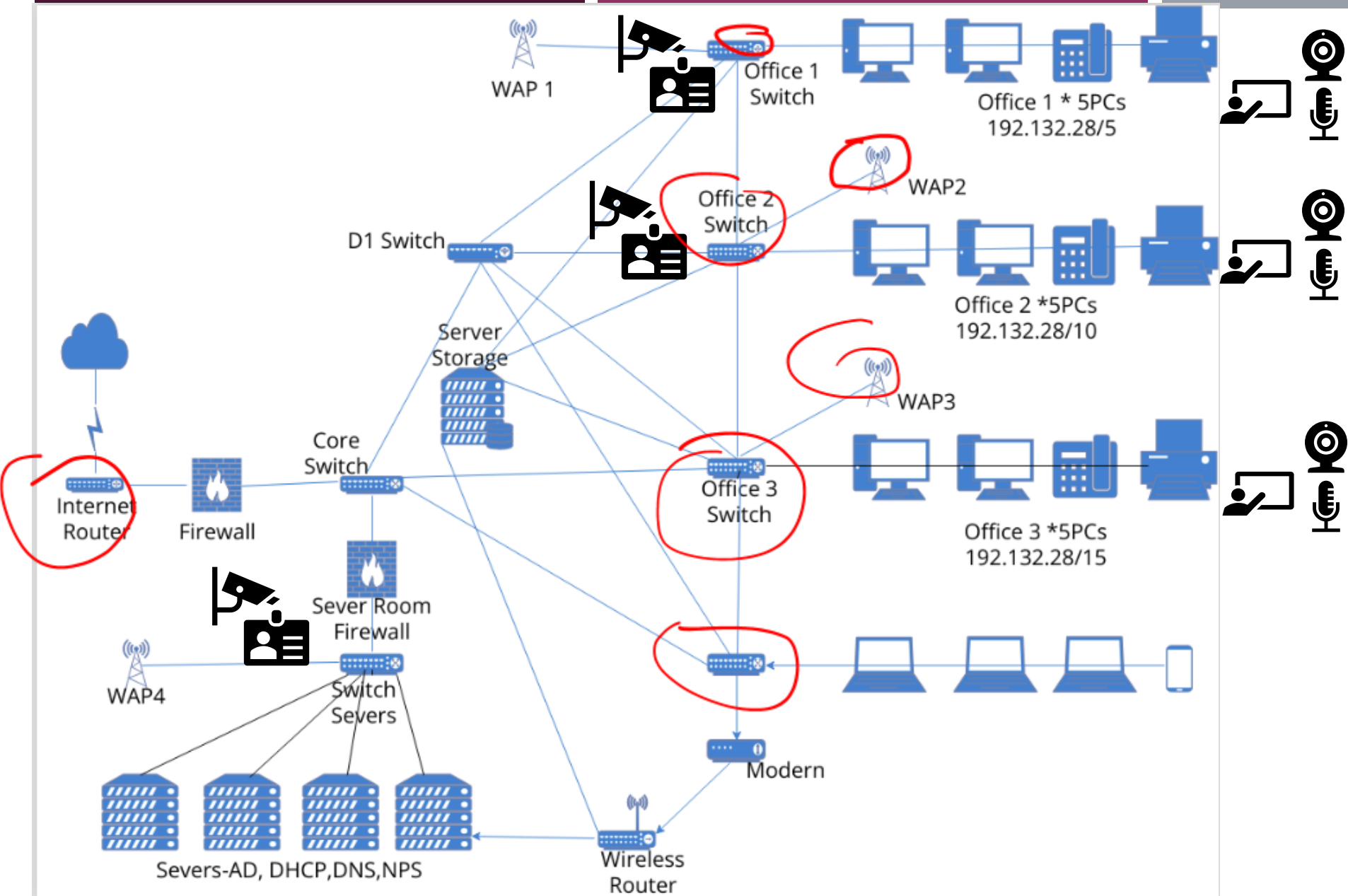
Office 3

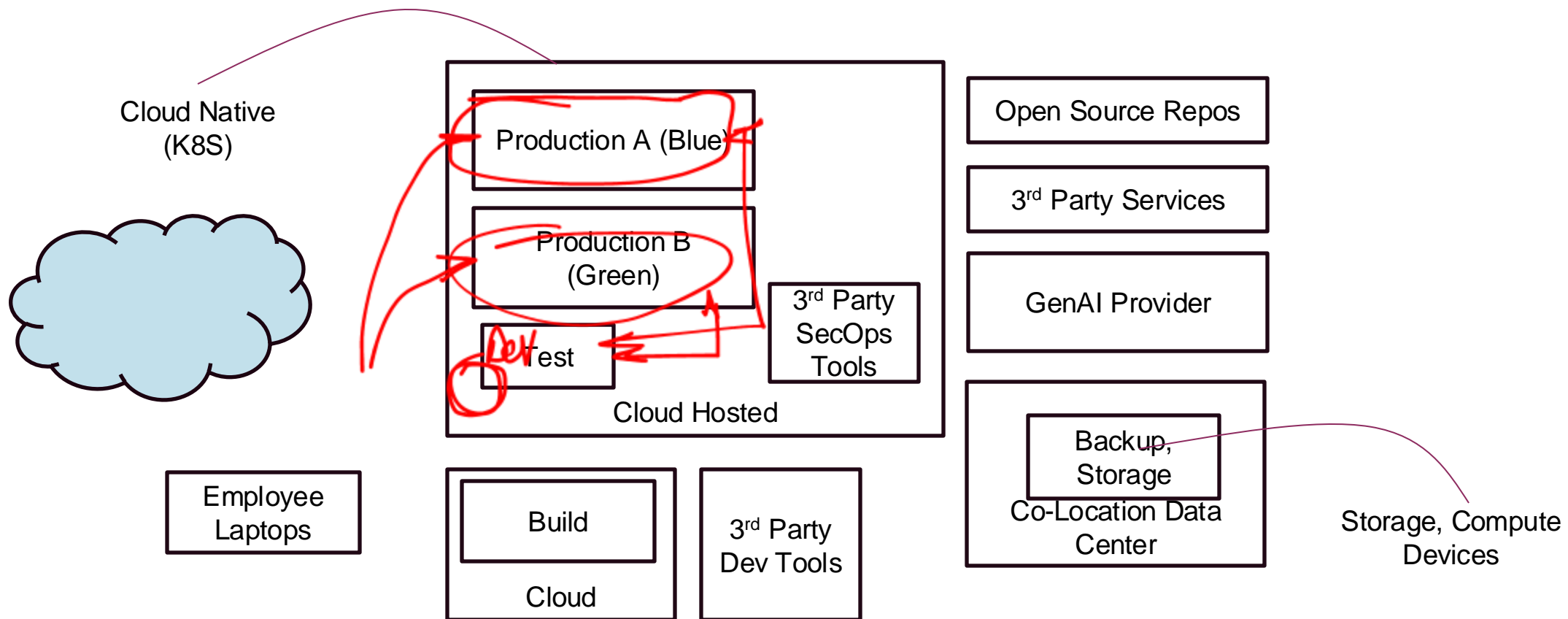


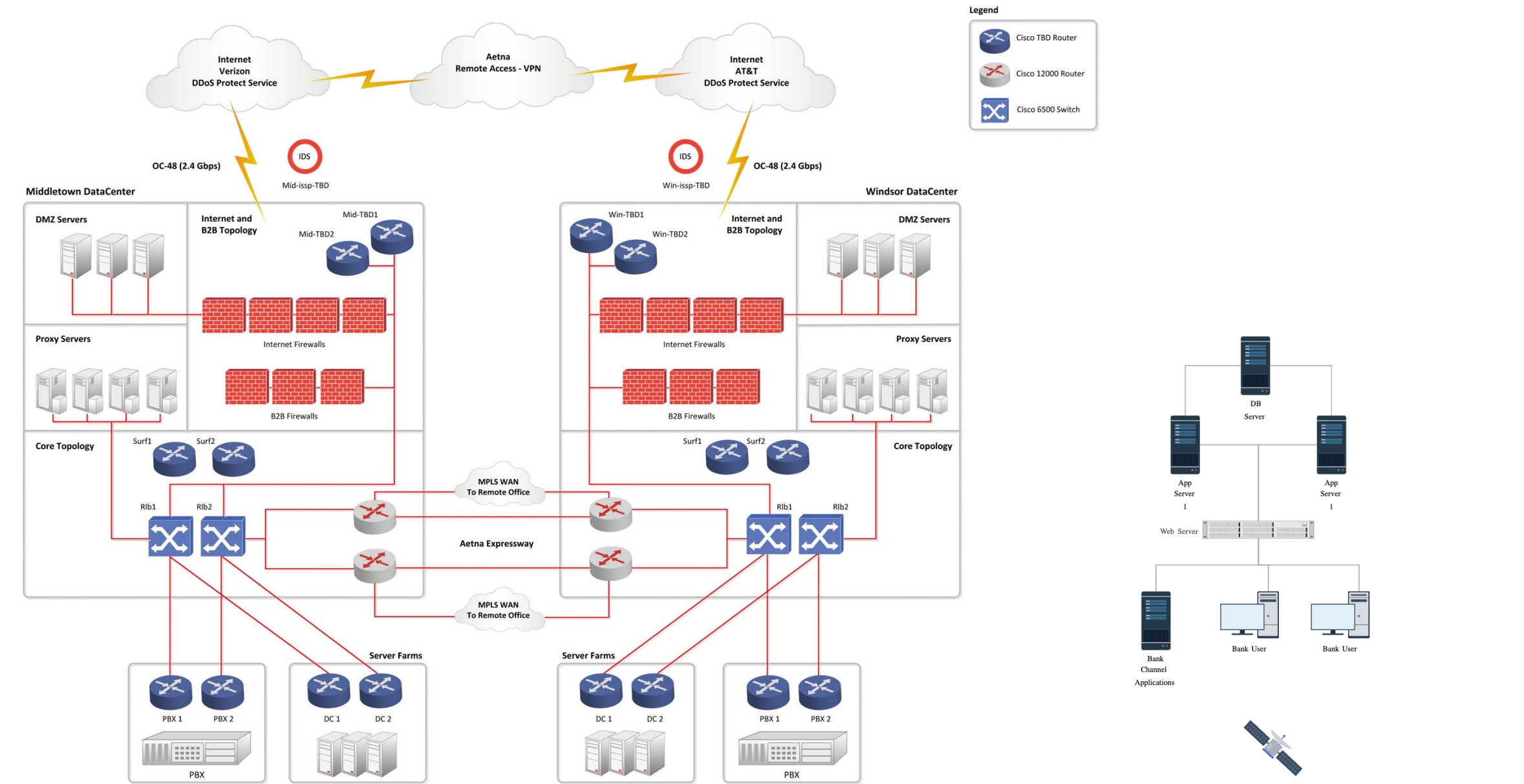
Local Server Room

Network Resilience

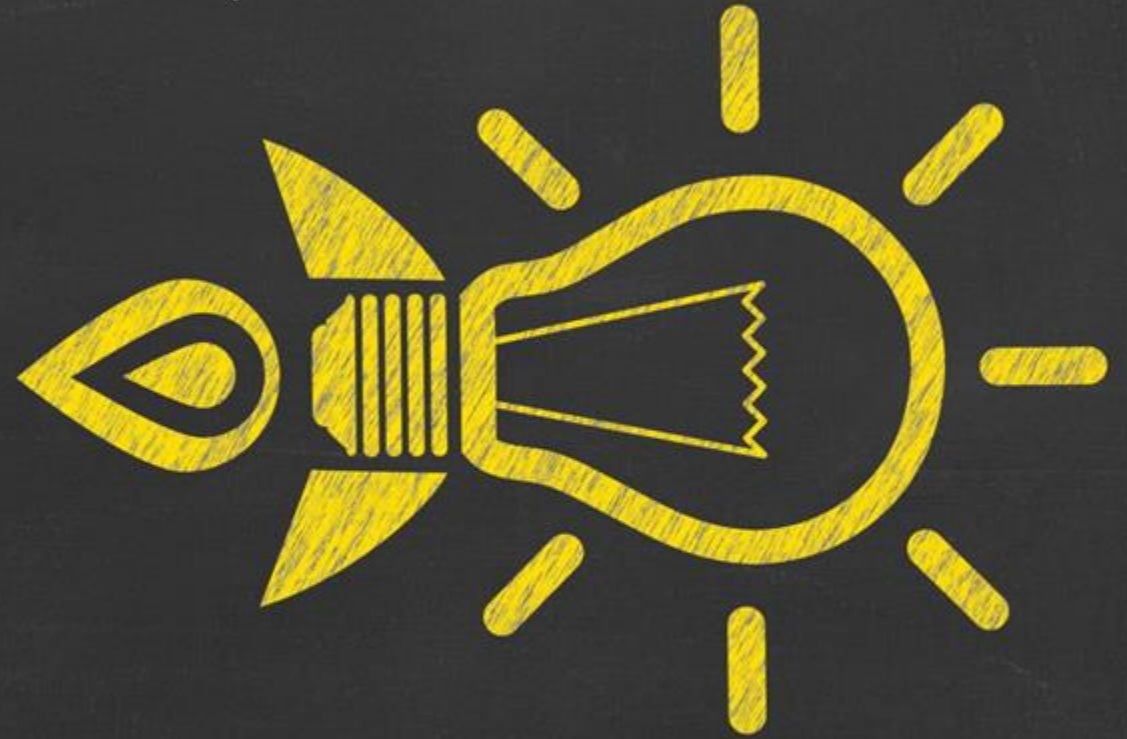
System designed to withstand disruptions, recover quickly from failures, and maintain operational continuity even during unexpected events



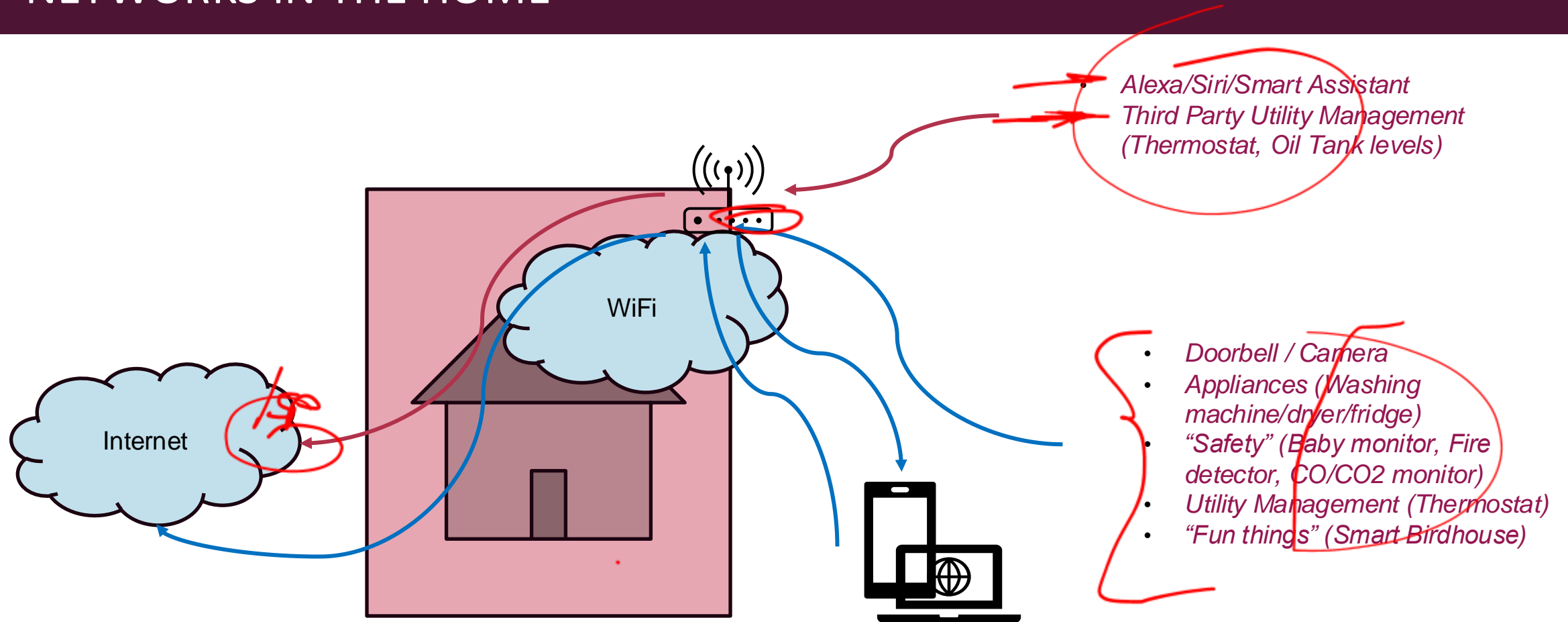




HOME NETWORKS (AND DEVICES)



NETWORKS IN THE HOME

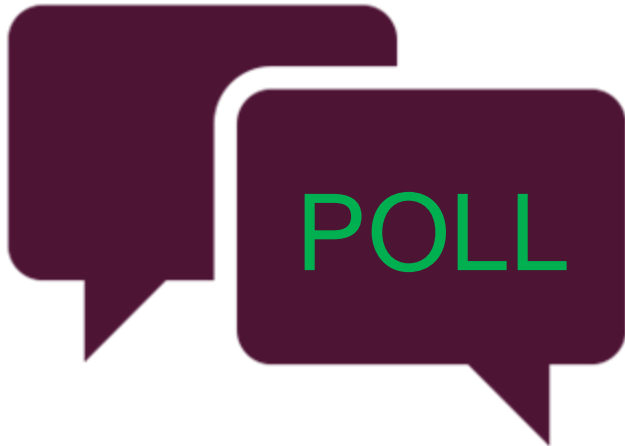


POLL PROMPT PART A



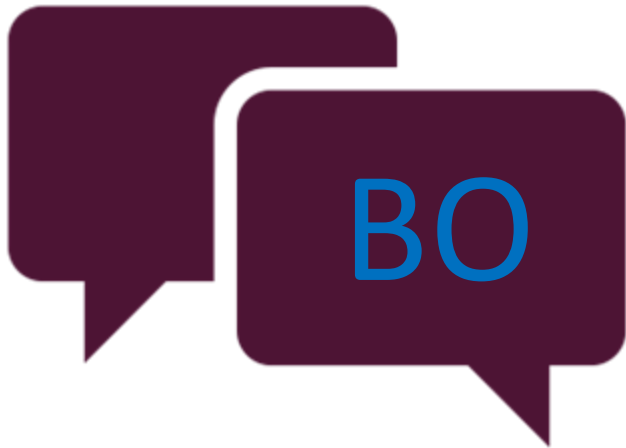
- How many of you have smart devices in your house...
 - Alexa/Siri/Smart Assistant
 - Doorbell / Camera
 - Appliances (Washing machine/dryer/fridge)
 - “Safety” (Baby monitor, Fire detector, CO/CO2 monitor)
 - Utility Management (Thermostat)
 - Third Party Utility Management (Thermostat, Oil Tank levels)
 - “Fun things” (Smart Birdhouse)
- How do you protect your networks / devices?
 - Segmentation based on authentication of users (for admin)
 - Reset all device passwords (including the ISP provided passwords)
 - Segmentation based on (mutual) authentication of devices (only known, approved devices allowed on your network)
 - Traffic management, logging traffic to/from your house and your ISP
 - Traffic management, monitoring traffic to/from your house and your ISP
 - Encryption of all traffic including between all these OT devices, your devices and your network router
- You are having a dinner party / gaming session / kids hanging out time at your house. Do you give everyone access to your network (give them the WiFi password)?
 - Yes
 - No
 - Yes but it's a separate guest network

POLL PROMPT PART B



- *Thinking about your home network and the discussion so far:*
- *What have you (implicitly or explicitly) used as the basis / discipline for protecting your home network*
 - *Network Segmentation*
 - *Network Traffic Management*
 - *Traffic Encryption*
 - *Network Resilience*
- *Totally unscientifically (we haven't defined maturity levels), what level would you assess your home network ZTA and protections at?*
 - *Basic (out of the box security)*
 - *Initial (starting to add protections)*
 - *Fit for purpose (confident you have hit ROI for effort to protect / risk to you & your family)*
 - *Optimal (best practices in place, protected against your kids & gaming friends & bad actors)*

BREAKOUT DISCUSSION: PRIORITIZATION



- *Hooray if you read the slides in advance...*
- *Given the results of the Poll, and the discussion from last week (both Breakout and Canvas about patching),*
 - *Are you confident in the protection of your home network?*
 - *If you think you have a "zero trust" home network, what is the basis of it?*
 - *How did thinking about your home network change how you might think about protecting a corporate network?*

CANVAS DISCUSSION: PRIORITIZATION

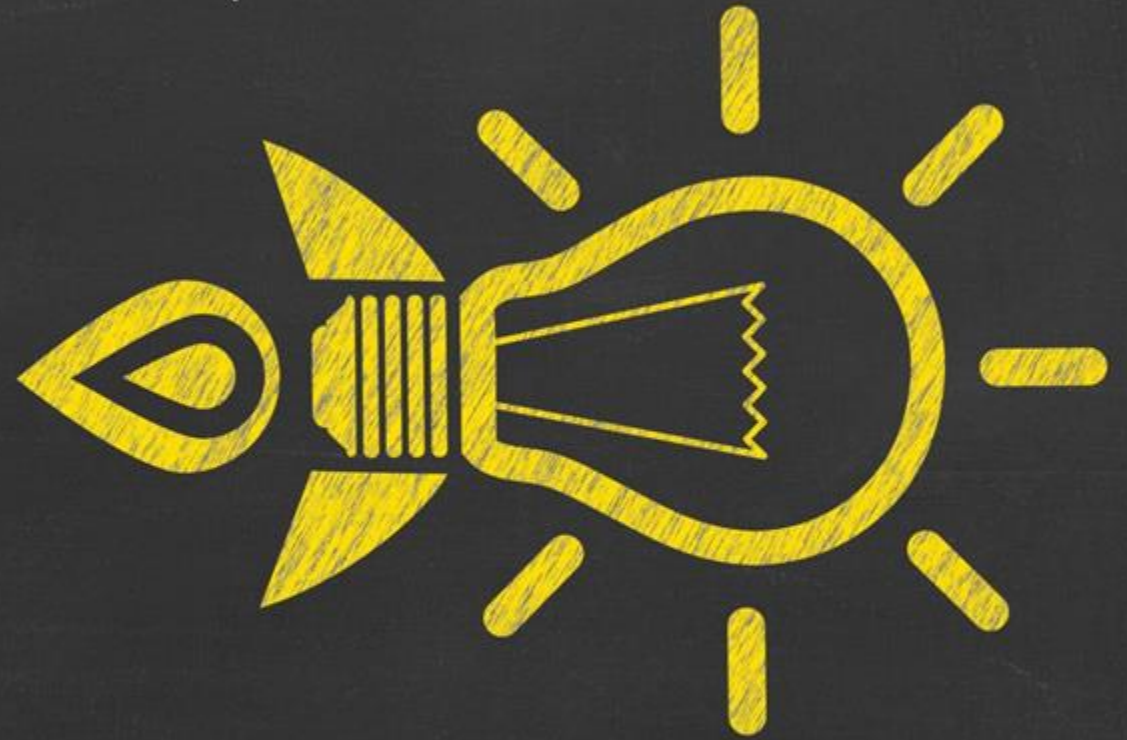


- *Based on the polls, breakouts and the remainder of the class, which do you think is more practical for you for protecting your home network, and why?*
 - *Following Secure by Design Pledge requirements (as in you follow them when managing your home network)*
 - *Adopting a Network ZTA mindset and moving up the maturity model path*

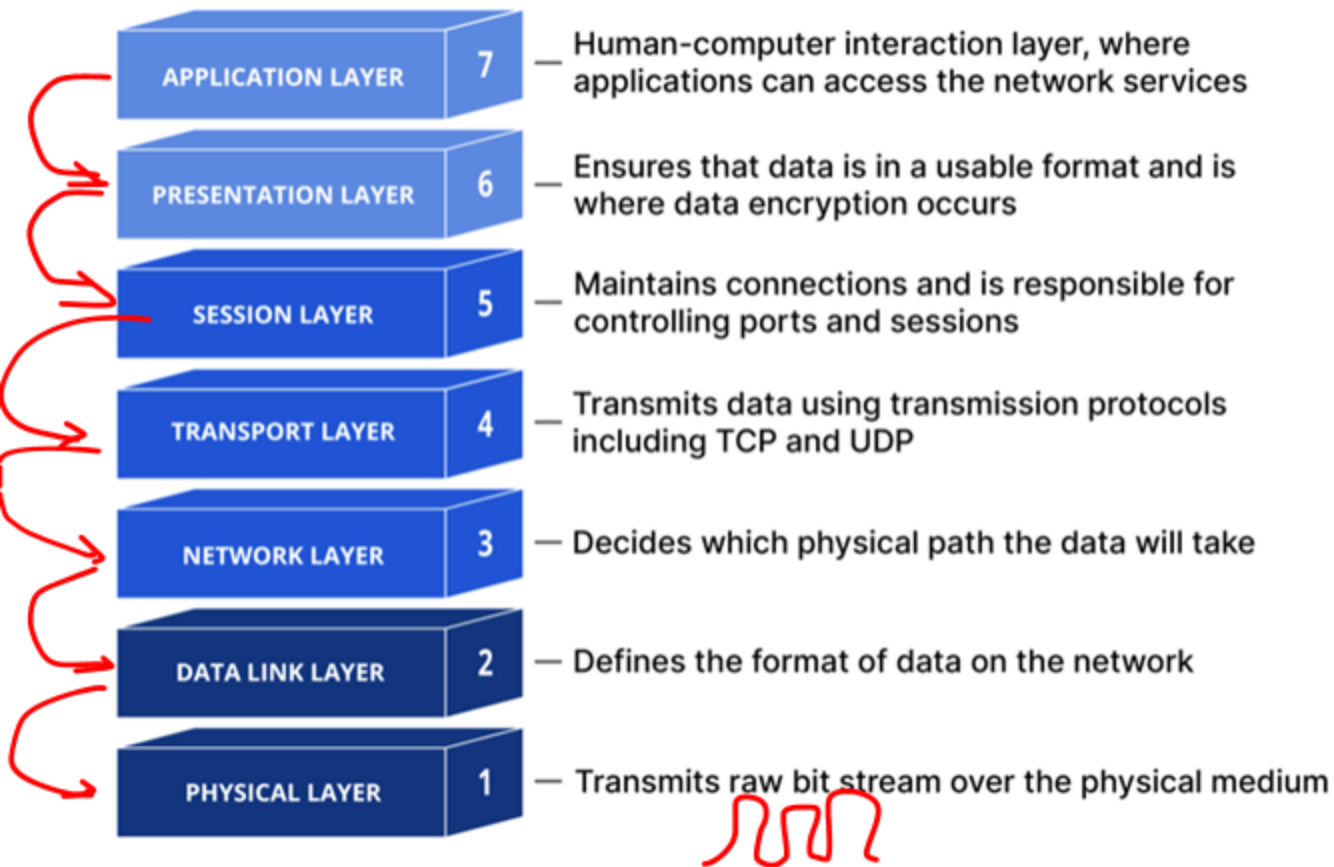


10 min
BREAK
BACK
6:20PM ET

NETWORK PROTOCOLS: NETWORK STACK



NETWORK STACK



TCP/IP Model



TCP/IP Protocol Suite



ATTACKS BY NETWORK STACK LAYER (BOTTOM UP)

- Layer 1 : Attack physical network components
- Layer 2 : Attack “operation” of protocols implemented at the (network) device level
- Layer 3 : Attack “operation” of (network / Internet) protocols implemented at the (system) device level
- Layer 4 : Attack “operation” of (Transport) protocols implemented at the (system) device level
- *Layer 3, 4 DDoS : Attacks that overwhelm devices by based on protocol behavior / response to inputs*
- Layer 5 : Attack “operation” of (session) protocols implemented at the (system, application) device level
- Layer 6 : Attack “operation” of (presentation) protocols implemented at the (system, application) device level
- Layer 7 : Attack “operation” of (presentation) protocols implemented at the (application) device level
- *Layer 7 DDoS : Attacks that overwhelm applications based on application behavior / response to inputs*

ATTACKS BY NETWORK STACK LAYER (TOP DOWN)

Attacks against the operation of protocols

- Layer 7: Presentation protocols implemented at the (application) device level
- Layer 6 : Presentation protocols implemented at the (system, application) device level
- Layer 5 : Session protocols implemented at the (system, application) device level
- Layer 4 : Transport protocols implemented at the (system) device level
- Layer 3 : Network / Internet protocols implemented at the (system) device level
- Layer 2 : Network protocols implemented at the (network) device level
- Layer 1 : Attack physical network components

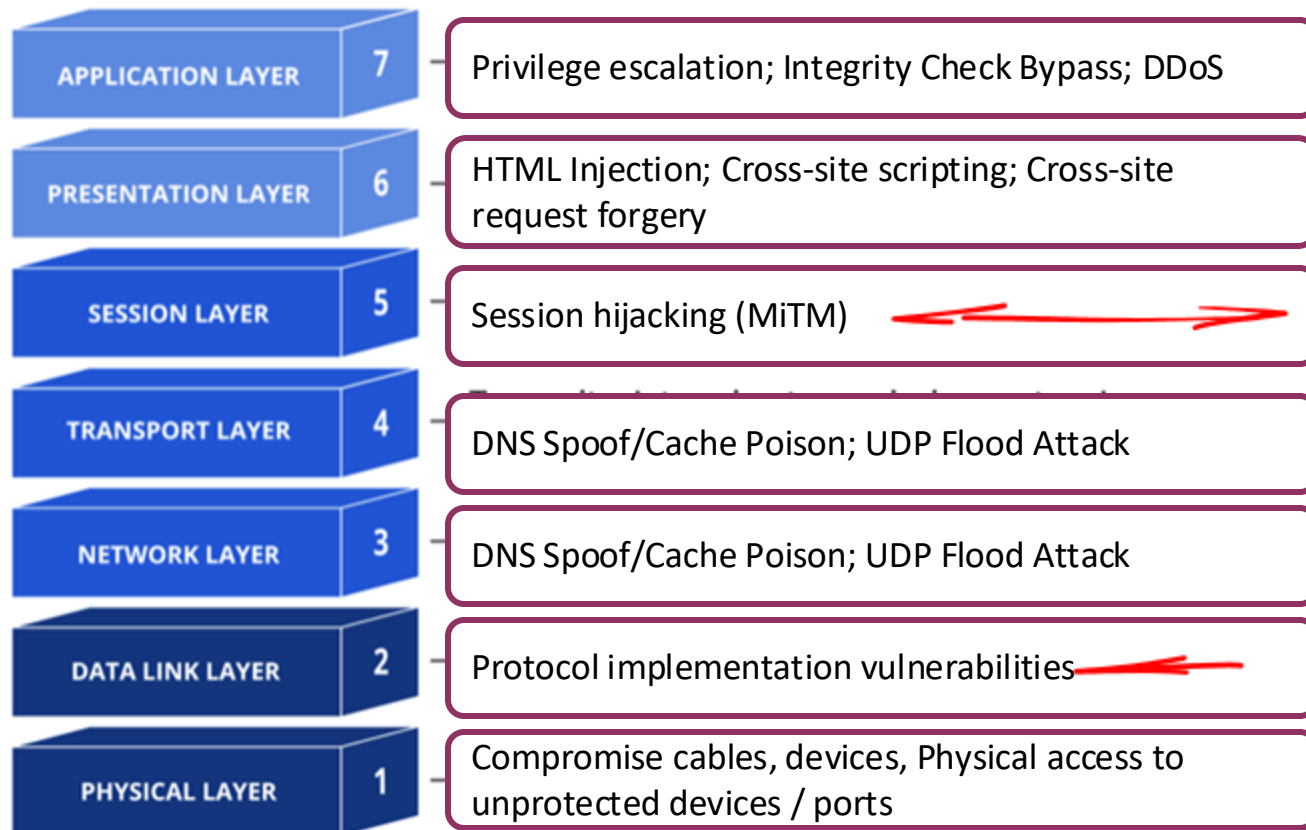
Attacks intended to overwhelm

- Layer 7 DDoS : Overwhelm applications based on application behavior / response to inputs
- Layer 3, 4 DDoS : Overwhelm devices by based on protocol behavior / response to inputs

NETWORK STACK

	Function	(Sample) Protocols
APPLICATION LAYER 7	Human Computer Interface (HCI) Layer, where applications access networks	FTP, HTTP, SMTP, TELNET, DNS
PRESENTATION LAYER 6	Ensures data in usable format; encryption is handled here	ASCII, PDF, HTML
SESSION LAYER 5	Maintains connections and is responsible for controlling ports and sessions	SQL, SIP, RFC-NAMED PIPES <i>SQLi</i>
TRANSPORT LAYER 4	Transmit data using transmission protocols including TCP, UDP	TCP, UDP, SSL, TLS
NETWORK LAYER 3	Decide which physical path the data will take	IP, ARP, IPSEC, ICMP, OSPF, BGP
DATA LINK LAYER 2	Define format of data on network	Ethernet, WIFI, 4G/5G
PHYSICAL LAYER 1	Transmit raw bit stream over physical medium	RS-232, RD34t, Ethernet, Wifi

NETWORK STACK



TCP/IP Model

Application Layer

Transport Layer

Internet Layer

Network Access Layer

TCP/IP Protocol Suite

HTTP
SMTP
Telnet
FTP
DNS
RIP
SNMP

TCP

UDP

ARP

IP

IGMP

ICMP

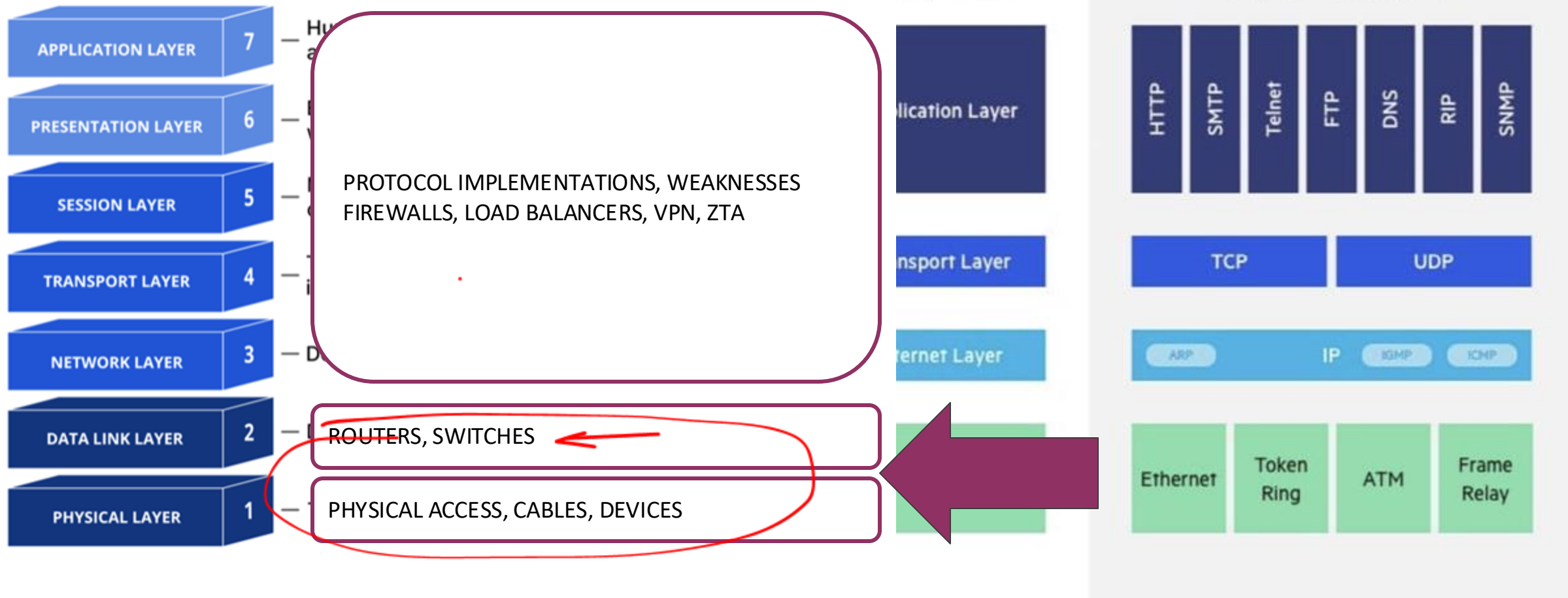
Ethernet

Token Ring

ATM

Frame Relay

NETWORK STACK



Layer	Protocols	Vulnerabilities (against protocols, implementations)	Attacks
Application	FTP, HTTP, SMTP, TELNET, DNS	CVE-1999-0082 (ftp CWD ~root) CVE-2023-48795 (SSH) HTTP/2 Rapid Reset	Privilege escalation Integrity Check Bypass DDoS
Presentation	ASCII, PDF, HTML	“Permissive” HTML Specification and improper sanitization: Anything XSS, XXSRF	HTML Injection Cross-site scripting Cross-site request forgery
Session	SQL, SIP, RFC-NAMED PIPES	Session layer protocol specifications CVE-2024-4249	Session hijacking (MiTM) SIP Protocol Implementation error
Transport	TCP, UDP, SSL, TLS	SSL specification : CVE-2014-3566 (POODLE) DNS Specification UDP specification	DNS Spoof/Cache Poison UDP Flood Attack
Network	IP, ARP, IPSEC, ICMP, OSPF, BGP	CVE-2022-20742 (F5 Big IP UDP Vulnerability)	UDP Flood (ICMP unreachable)
Data	Ethernet, WIFI, 4G/5G	Wifi: Not configured for security	
Physical	RS-232, RS-485, Network (Ethernet) ports	RS-232 : Lack of Encryption, Authentication	Physical access / Impersonation Compromise cables, devices

IN THE NEWS: WIFI VULNERABILITIES



WIFI VULNERABILITIES

- https://www.theregister.com/2023/03/30/wifi_spec_ambiguity_leak/
 - **Warning: Your wireless networks may leak data thanks to Wi-Fi spec ambiguity**
- <https://papers.mathyvanhoef.com/usenix2023-wifi.pdf>
 - The Wi-Fi standard (IEEE 802.11) is not specific enough about how to handle buffered frames
 - This is vulnerability at the network protocol level
- <https://arstechnica.com/security/2024/01/chinese-malware-removed-from-soho-routers-after-fbi-issues-covert-commands/>
 - Chinese malware removed from SOHO routers after FBI issues covert commands
 - The routers—mainly Cisco and Netgear devices that had reached their end of life—were infected with what's known as KV Botnet malware
 - This is a vulnerability at the network device level

IN THE NEWS: ETERNAL BLUE: WANNACRY, NOTPETYA



ETERNALBLUE, WANNACRY, PETYA

<https://www.sentinelone.com/blog/eternalblue-nsa-developed-exploit-just-wont-die/>

What is Eternalblue?

- CVE-2017-0143 to CVE-2017-0148 are a family of critical vulnerabilities in Microsoft SMBv1 server & protocol (so storage not network but it's a protocol) used in Windows 7, Windows Server 2008, Windows XP and even Windows 10 running on port 445.
- Eternalblue itself concerns [CVE-2017-0144](#), a flaw that allows remote attackers to execute arbitrary code on a target system by sending specially crafted messages to the SMBv1 server.
- The flaws in SMBv1 protocol were patched by Microsoft in March 2017 with the [MS17-010](#) security update.
 - Unfortunately, despite the patch being available for more than 2 years, there are still reportedly around a million machines connected to the internet that remain vulnerable.

WANNACRY

- <https://www.justice.gov/archives/opa/pr/north-korean-regime-backed-programmer-charged-conspiracy-conduct-multiple-cyber-attacks-and-https://web.archive.org/web/20170711015125/https://nakedsecurity.sophos.com/2017/05/17/wannacry-the-ransomware-worm-that-didnt-arrive-on-a-phishing-hook/>
 - To guard against malware exploiting Microsoft vulnerabilities:
 - Stay on top of all patch releases and apply them quickly.
 - If at all possible, replace older Windows systems with the latest versions.
- <https://www.cloudflare.com/learning/security/ransomware/wannacry-ransomware/>
 - WannaCry showed that unless a network is air-gapped — meaning it is completely separate from all outside connections — external threats can likely still get in.
 - **Even patched vulnerabilities can be dangerous.** A vulnerability patch is only as effective as the number of systems that apply it.

PETYA, NOT PETYA

- WannaCry, Petya, NotPetya are all ransomware
- NotPetya and WannaCry included/depended on the Eternalblue vulnerability
 - Notably, NotPetya was observed using the same EternalBlue vulnerability ([CVE-2017-0144](#)) that the worldwide [WannaCry attack](#) had used earlier in 2017.
 - This enabled it to spread rapidly across networks without any intervention from users
 - Microsoft issued a patch for the EternalBlue vulnerability in March 2017, but many organizations had not installed the patch.
- Petya used/depended on opening an infected email attachment
 - Petya spreads mostly through email attachments. Attackers send emails to HR departments with fake job applications attached. The attached PDFs either [contain an infected Dropbox link](#) or are [actually executable files in disguise](#) — depending on the attack method used.

NOT PETYA

EDR
BE

N.S.

IN THE NEWS: POODLE



POODLE

<https://www.cisa.gov/news-events/alerts/2014/10/17/ssl-30-protocol-vulnerability-and-poodle-attack>

DESERT
DISABLE

- **SSL 3.0 Protocol Vulnerability and POODLE Attack**
- US-CERT is aware of a **design vulnerability** found in the way SSL 3.0 handles block cipher mode padding. The POODLE attack demonstrates how an attacker can exploit this vulnerability to decrypt and extract information from inside an encrypted transaction.
- While SSL 3.0 is an old encryption standard and has generally been replaced by TLS, most SSL/TLS implementations remain backwards compatible with SSL 3.0 to interoperate with legacy systems in the interest of a smooth user experience.
- There is currently no fix for the vulnerability SSL 3.0 itself, as the issue is fundamental to the protocol; however, disabling SSL 3.0 support in system/application configurations is the most viable solution currently available.

IN THE NEWS: NETWORK TRAFFIC MANAGEMENT, NETWORK RESILIENCE DDOS WITH HTTP/2 RAPID RESET

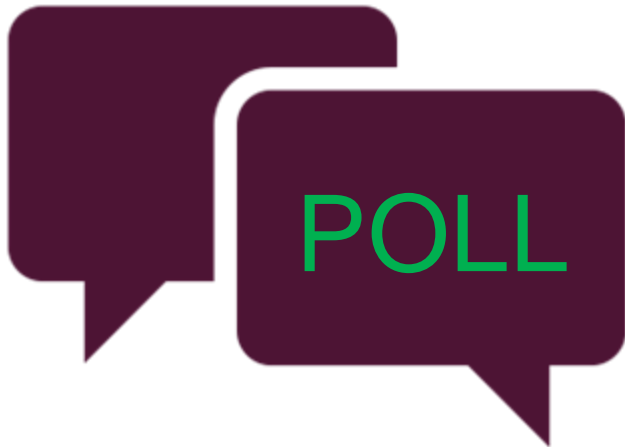


DDOS WITH NETWORK PROTOCOLS VULNERABILITY

<https://cloud.google.com/blog/products/identity-security/how-it-works-the-novel-http2-rapid-reset-ddos-attack>

- <https://nvd.nist.gov/vuln/detail/CVE-2023-44487>
- A novel HTTP/2-based DDoS attack peaked in August 2023.
 - These attacks were significantly larger than any previously-reported Layer 7 attacks, with the largest attack surpassing 398 million requests per second.
- One of the main constraints when mounting a Layer 7 DoS attack is the number of concurrent transport connections.
 - In HTTP/1.1, each request is processed serially. The server will read a request, process it, write a response, and only then read and process the next request.
 - With HTTP/2, the client can open multiple concurrent streams on a single TCP connection, each stream corresponding to one HTTP request.
- This attack is called Rapid Reset because it relies on the ability for an endpoint to send a RST_STREAM frame immediately after sending a request frame → this makes the other endpoint start working and then rapidly resets the request. The request is canceled, but the HTTP/2 connection is left open, leading to resource exhaustion

POLL PROMPT – THREATS



- *How many of you were involved in remediation activities related to*
 - *Poodle / SSLv3*
 - *EternalBlue/WannaCry*
 - *EternalBlue/NotPetya*
 - *Petya*
 - *HTTP/2 Rapid Reset*
 - *Anything related to a SOHO/Home router*
- *Which do you think poses the great threat to your business :*
 - *Protocol vulnerabilities (including SMB, SSH/TLS, WiFi, HTTP/2)*
 - *Poodle (SSL v3)*
 - *Think Eternal Blue leading to NotPetya, WannaCry*
 - *HTTP/2*
 - *User managed network devices (such as at home routers as part of allowing users to work from home)*
 - *SOHO Routers as in the news*

CLASS DISCUSSION: PRIORITIZATION

CLASS

- *For those of you who were involved / around / aware of the impact of Poodle, WannaCry, Not Petya in their organizations (not just in the news), what changed in your organization after?*
- *Did you have organization-wide efforts to*
 - *Identify inventory of workstations, servers, patched/unpatched systems?*
 - *Identify inventory of applications using SSLv3, HTTP/2*
 - *Upgrade your customer-facing products away from SSLv3, HTTP/2?*
- *What was the most impactful thing your organization did to improve its security as a result of this?*
- *What about HTTP/2 Rapid Reset – who was involved and what did your response look like?*

INVENTORY
PATCHES



ANTICIPATED END OF LECTURE 3

