2022

Class #7 – Domain 4

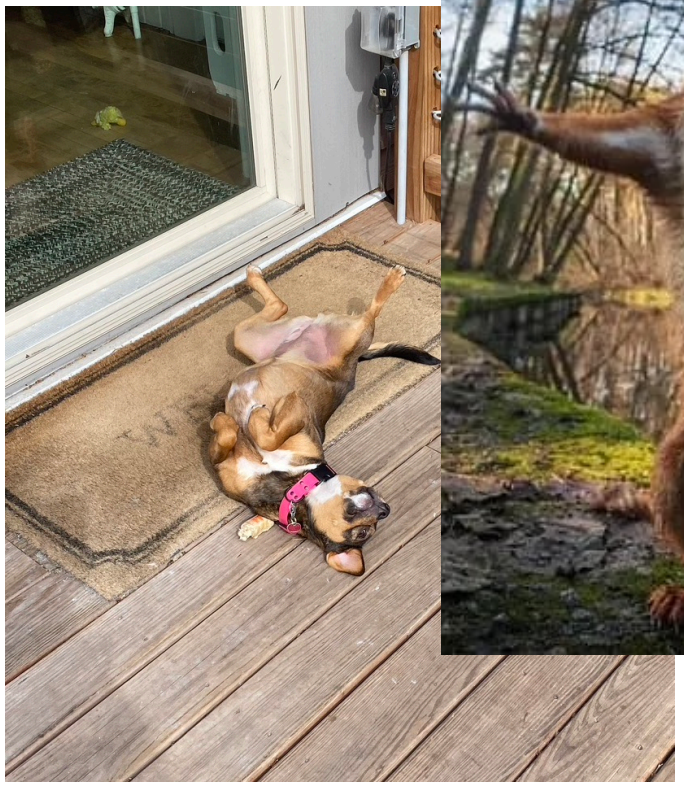
Evan Francen

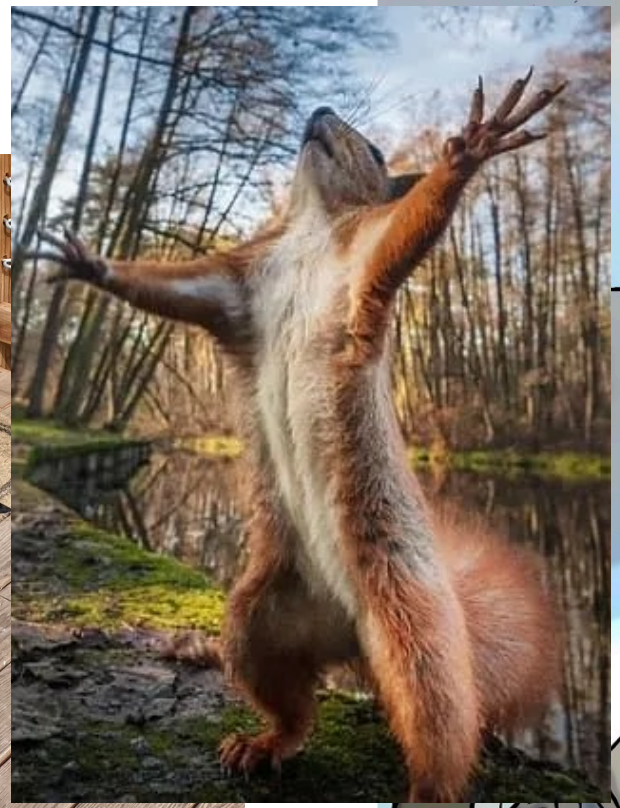
Evan Francen – FRSecure and SecurityStudio Co-Founder & CEO

CISSP® MENTOR PROGRAM – SESSION SEVEN

I'M BACK!

Lucky you...





CISSP® MENTOR PROGRAM – SESSION SEVEN

INTRODUCTION

Agenda

- Welcome, Reminders, & Introduction
- Questions
- **Domain 4 – Communication and Network Security (pp. 334 - Kindle)**
  - Review (a little).
  - Cheat Sheet
  - **Secure Network Components**
  - **Implement Secure Communication Channels According to Design**

CISSP® MENTOR PROGRAM – SESSION SEVEN

INTRODUCTION
Agenda

Some testable goodies tonight!

- Welcome, Reminders, & Introduction
- Questions
- **Domain 4 – Communication and Network Security (pp. 334 - Kindle)**
  - Review (a little).
  - Cheat Sheet
  - **Secure Network Components**
  - **Implement Secure Communication Channels According to Design**

CISSP® MENTOR PROGRAM – SESSION SEVEN

FRSECURE CISSP MENTOR PROGRAM LIVE STREAM

THANK YOU!

Quick housekeeping reminder.

- The online/live chat that's provided while live streaming on YouTube is for constructive, respectful, and relevant (about course content) discussion **ONLY**.
- At **NO TIME** is the online chat permitted to be used for disrespectful, offensive, obscene, indecent, or profane remarks or content.
- Please do not comment about controversial subjects, and please **NO DISCUSSION OF POLITICS OR RELIGION**.
- Failure to abide by the rules may result in disabling chat for you.
- **DO NOT** share or post copywritten materials. (pdf of book)

CISSP® MENTOR PROGRAM – SESSION SEVEN

GETTING GOING…

Managing Risk!

Study Tips:

- Study in small amounts frequently (20-30 min)
- Flash card and practice test apps help
- Take naps after heavy topics (aka Security Models)
- Write things down, say them out loud
- Use the Slack Channels
- Exercise or get fresh air in between study sessions

CISSP® MENTOR PROGRAM – SESSION SEVEN

GETTING GOING…

Managing Risk!

Study Tips:

- Study in small amounts frequently (20-30 min)
- Flash card and practice test apps help
- Take naps after heavy topics (aka Security Models)
- Write things down, say them out loud
- Use the Slack Channels
- Exercise or get fresh air in between study sessions

Stick with it. You'll be glad you did. I promise.

CISSP® MENTOR PROGRAM – SESSION SEVEN

GETTING GOING…
THANK YOU!

- **Christophe** pretty much kicked butt on Monday. Got us caught up with the schedule.
- **Ryan** is keeping us all sane(ish).
- **Ron** is EL MEJOR PROFESOR!
- **Brandon Matis** (you don't get to see him, but he makes most of this happen).
- Many unsung **FRSecure heroes** doing heroey things.

GET
THA

- Chr
  Got
- Rya
- Ror
- Bra
  ma
- Mar
  thir

day.

he

y

CISSP® MENTOR PROGRAM – SESSION SEVEN

GETTING GOING…
THANK YOU!

- **Christophe** pretty much kicked butt on Monday. Got us caught up with the schedule.

Speaking of this…

He covered **a lot of material** and some of it may seem

CISSP® MENTOR PROGRAM – SESSION SEVEN

GETTING GOING…
THANK YOU!

- **Christophe** pretty much kicked butt on Monday. Got us caught up with the schedule.

Speaking of this…

He covered **a lot of material** and some of it may seem

CISSP® MENTOR PROGRAM – SESSION SEVEN

GETTING GOING…
THANK YOU!

- **Christophe** pretty much kicked butt on Monday. Got us caught up with the schedule.

Speaking of this…

He covered **a lot of material** and some of it may seem

Encryption

CISSP® MENTOR PROGRAM – SESSION SEVEN

GETTING GOING…
THANK YOU!

- **Christophe** pretty much kicked butt on Monday. Got us caught up with the schedule.

Speaking of this…

He covered **a lot of material** and some of it may seem

Cryptographic Methods

Encryption

CISSP® MENTOR PROGRAM – SESSION SEVEN

GETTING GOING…
THANK YOU!

- **Christophe** pretty much kicked butt on Monday. Got us caught up with the schedule.

Symmetric Encryption

…this…

He covered **a lot of material** and some of it may seem

Cryptographic Methods

Encryption

CISSP® MENTOR PROGRAM – SESSION SEVEN

GETTING GOING…
THANK YOU!

- Christop… …h kicked butt on Monday. Got us ca… …he schedule.

Asymmetric Encryption

Symmetric Encryption

…this…

He covered a lot of material and some of it may seem

Cryptographic Methods

Encryption

CISSP® MENTOR PROGRAM – SESSION SEVEN

GETTING GOING…
THANK YOU!

- Christop… …h kicked butt on Monday. Got us ca… …he schedule.

Asymmetric Encryption

Symmetric Encryption

…his…

He covered a lot of material and some of it may seem

Cryptographic Methods

Encryption

Quantum Cryptography

CISSP® MENTOR PROGRAM – SESSION SEVEN

GETTING GOING…
THANK YOU!

- Christop… …h kicked butt on Monday. Got us ca… …he schedule

Asymmetric Encryption

Symmetric Encryption

PKI

…his…

He covered a lot of material and some of it may seem

Cryptographic Methods

Encryption

Quantum Cryptography

GETTING GOING…

THANK YOU!

Digital Signatures and Digital Certificates

- Christop… kicked butt on Monday. Got us ca… the schedule

Asymmetric Encryption

Symmetric Encryption

PKI

…his…

He covered a lot of material and some of it may seem

Cryptographic Methods

Encryption

Quantum Cryptography

CISSP® MENTOR PROGRAM – SESSION SEVEN

GETTING GOING…

THANK YOU!

- Christop… …h kicked butt on Monday. Got us ca… …he schedule

Digital Signatures and Digital Certificates

Asymmetric Encryption

Symmetric Encryption

PKI

…his…

He covered a lot of material and some of it may seem

Cryptographic Methods

Encryption

Hash Functions

Quantum Cryptography

GETTING GOING…
THANK YOU!

- Christop… …h kicked butt on Monday. Got us ca… …he schedule
- He covered a l… …e of it may seem

Digital Signatures and Digital Certificates

Asymmetric Encryption

Symmetric Encryption

PKI

Cryptanalytic Attacks

Cryptographic Methods

Encryption

Hash Functions

Quantum Cryptography

CISSP® MENTOR PROGRAM – SESSION SEVEN

GETTING GOING…

THANK YOU!

- Christop… …h k…ed butt on Monday.
  Got us ca… …he s…dule
  …chi…
  He covered a l… …e of it may seem

Digital Signatures and Digital Certificates

Asymmetric Encryption

Symmetric Encryption

PKI

Cryptanal… …acks

Cryptographic Methods

Encryption

Hash Functions

Quantum Cryptography

GETTING GOING...

Site and Facility Design

Digital Signatures and
tes

Asymmetric Encryption

Symmetric Encryption

PKI

Cryptanal acks

Cryptographic Methods

Encryption

Hash Functions

Quantum Cryptography

GETTING GOING...

Site and Facility Design

Digital Signatures and
tes

Site and Facility
Security Controls

Asymmetric
Encryption

Symmetric
Encryption

PKI

Cryptanal acks

Cryptographic
Methods

Encryption

Hash Functions

Quantum
Cryptography

GETTING GOING...

Site and Facility Design

Digital Signatures and

tes

Asymmetric Encryption

Site and Facility Security Controls

Symmetric Encryption

PKI

Restricted and Work Area Security

Cryptographic Methods

Encryption

Hash Functions

Quantum Cryptography

GETTING GOING...

Site and Facility Design

Digital Signatures and

tes

Site and Facility Security Controls

Utilities and Heating, Ventilation, and Air Conditioning

Symm

Encryption

PKI

Restricted and Work Area Security

anal acks

e of it may

Cryptographic Methods

Encryption

Hash Functions

Quantum Cryptography

GETTING GOING...

Site and Facility Design

Digital Signatures and

tes

Site and Facility Security Controls

Utilities and Heating, Ventilation, and Air Conditioning

Symm

Encryption

PKI

Restricted and Work Area Security

anal acks

e of it may

Cryptographic Methods

Fire Prevention, Detection, and Suppression

Encryption

Hash Functions

Quantum Cryptography

GETTING GOING…

Site and Facility Design

Digital Signatures and

tes

Site and Facility Security Controls

Utilities and Heating, Ventilation, and Air Conditioning

Symm

Encryption

PKI

Restricted and Work Area Security

e of it may

Cryptographic

Fire Prevention, Detection, and Suppression

But wait, there's more!!!

Hash Functions

Cryptography

Domain 4: Communication and Network Security

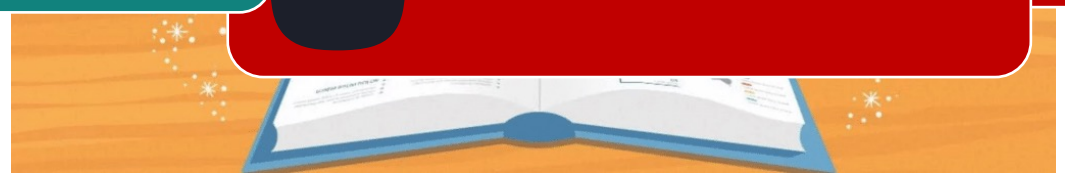
Domain 4: Communication and Network Security

Network Defense-in-Depth

Restricted and Work Area Security

Fire Prevention, Detection, and Suppression

But wait, there's more!!!



Domain 4: Communication and Network Security

Network Defense-in-Depth

Restricted and Work Area Security

Fire Prevention, Detection, and Suppression

But wait, there's more!!!

LANs, WANs, MANs, GANs, PANs…

Domain 4: Communication and Network Security

Network Defense-in-Depth

Restricted and Work Area Security

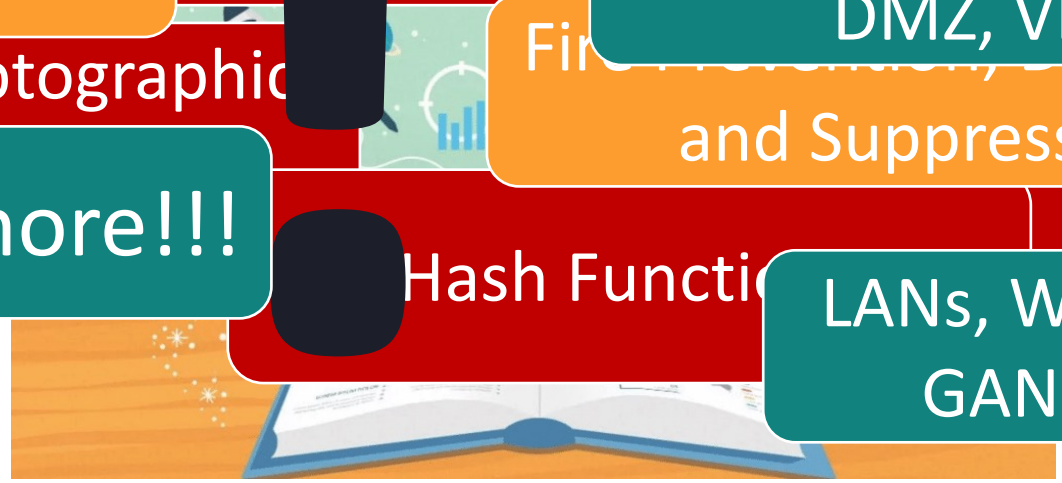
But wait, there's more!!!

PKI

Internet, intranet, extranet, DMZ, VLAN, SDN

and Suppression

LANs, WANs, MANs, GANs, PANs...



Domain 4: Communication and Network Security

Network Defense-in-Depth

PKI

The OSI Model

Restricted and Wor
Area Security

Internet, intranet, extranet,
DMZ, VLAN, SDN

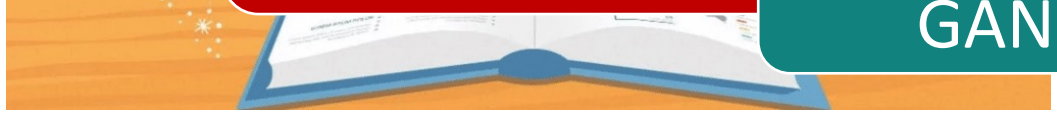
Cryptographic

and Suppression

But wait, there's more!!!

Hash Functi

LANs, WANs, MANs,
GANs, PANs...



Domain 4: Communication and Network Security

Network Defense-in-Depth

The TCP/IP Model

PKI

The OSI Model

Restricted and Wor… Area Security

Internet, intranet, extranet, DMZ, VLAN, SDN

Cryptographic…

…and Suppression

But wait, there's more!!!

Hash Functi…

LANs, WANs, MANs, GANs, PANs…

Domain 4: Communication and Network Security

Network Defense-in-Depth

The TCP/IP Model

The OSI Model

Restricted and Wor… Area Security

Internet, intranet, extranet, DMZ, VLAN, SDN

Cryptographic…

…and Suppression

But wait, there's more!!!

Encapsulation

LANs, WANs, MANs, GANs, PANs…

Domain 4: Communication and Network Security

Network Defense-in-Depth

The TCP/IP Model

The OSI Model

Internet, intranet, extranet, DMZ, VLAN, SDN

IPv4

and Suppression

But wait, there's more!!!

Encapsulation

LANs, WANs, MANs, GANs, PANs...

Domain 4: Communication and Network Security

Network Defense-in-Depth

The TCP/IP Model

PKI

The OSI Model

IPv6

Internet, intranet, extranet, DMZ, VLAN, SDN

IPv4

and Suppression

But wait, there's more!!!

LANs, WANs, MANs, GANs, PANs...

Encapsulation

Domain 4: Communication and Network Security

Network Defense-in-Depth

Network attacks

The TCP/IP Model

IPv6

The OSI Model

Internet, intranet, extranet, DMZ, VLAN, SDN

IPv4

and Suppression

But wait, there's more!!!

Encapsulation

LANs, WANs, MANs, GANs, PANs...

Domain 4: Communication and Network Security

Network Defense-in-Depth

Network attacks

The TCP/IP Model

IPv6

The OSI Model

Internet, intranet, extranet, DMZ, VLAN, SDN

IPv4

Secure Protocols

But wait, there's more!!!

Encapsulation

LANs, WANs, MANs, GANs, PANs...

Domain 4: Communication and Network Security

Microsegmentation

Network Defense-in-Depth

Network attacks

The TCP/IP Model

The OSI Model

IPv6

IPv4

Internet, intranet, extranet, DMZ, VLAN, SDN

Secure Protocols

But wait, there's more!!!

Encapsulation

LANs, WANs, MANs, GANs, PANs...

Domain 4: Communication and Network Security

Microsegmentation

Network Defense-in-Depth

Network attacks

The TCP/IP Model

IPv6

The OSI Model

Internet, intranet, extranet, DMZ, VLAN, SDN

IPv4

Secure Protocols

Wireless Networks

But wait, there's more!!!

Encapsulation

LANs, WANs, MANs, GANs, PANs...

Domain 4: Communication and

Micros

P

et,

s

Networks

But wait, there's more!!!

Hash Functi

Encapsulation

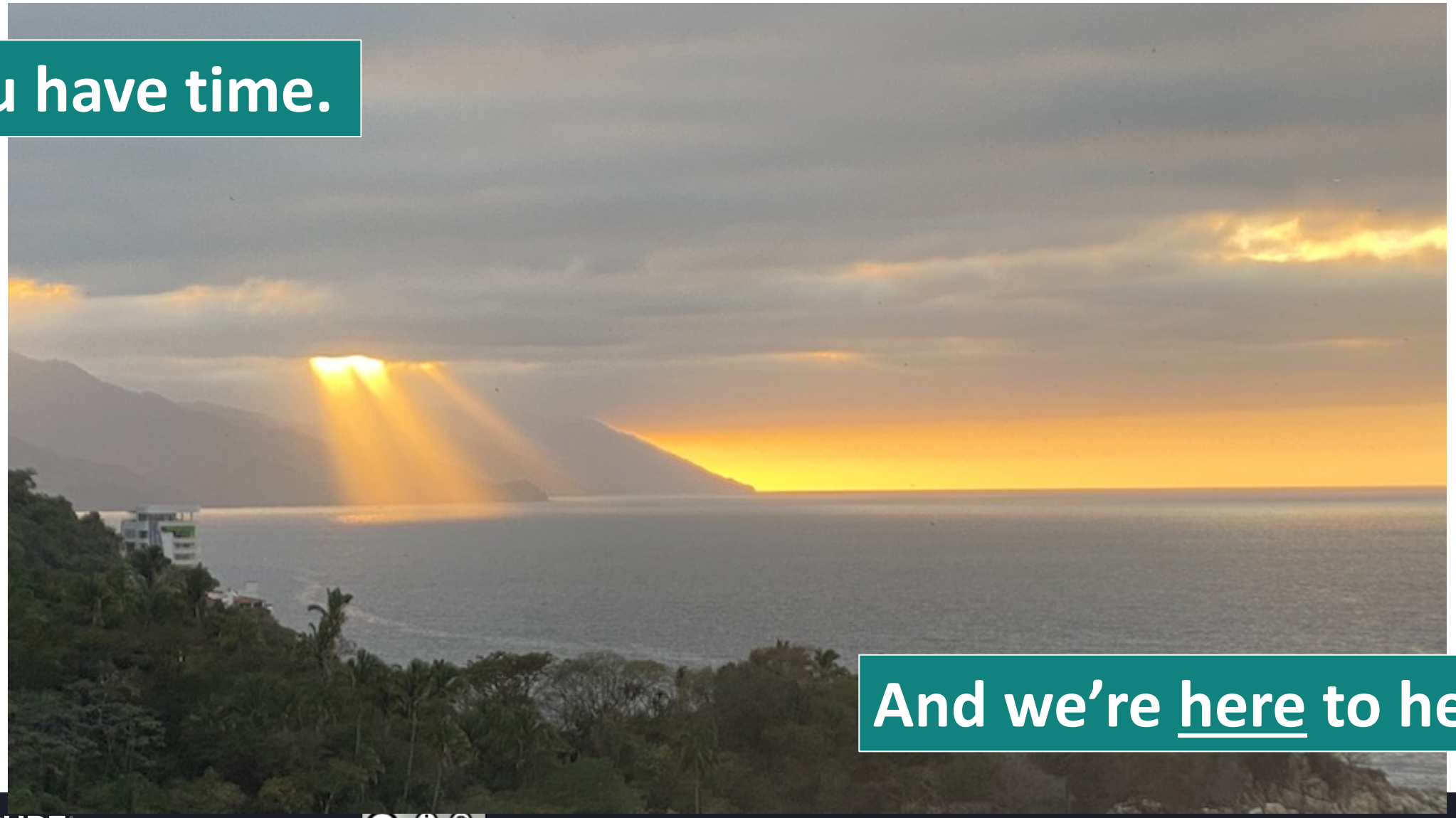
LANs, WANs, MANs, GANs, PANs…

Where you at all overwhelmed?!

CISSP® MENTOR PROGRAM – SESSION SEVEN

RELAX

RELAX



INTRODUCTION
Agenda

Some testable goodies tonight!

- ~~Welcome, Reminders, & Introduction~~
- Questions
- **Domain 4 – Communication and Network Security (pp. 334 - Kindle)**
  - Review (a little).
  - Cheat Sheet
  - **Secure Network Components**
  - **Implement Secure Communication Channels According to Design**

QUESTIONS.

The most common questions:

Check your email for links

- **Slack channel** - Use it for more in-depth questions / discussions
- Live session links & Recording
- Instructor slide deck
- Other Resources

CISSP® MENTOR PROGRAM – SESSION SEVEN

QUESTIONS.

The most common questions:

C C May 5th at 7:02 AM

Good Morning ☀️ I have a question ❓

can a security assessment based on risk (low/mid/high) serve as threat modeling? Also, is it possible to get examples of a threat model, security plan and due diligence plan so we can visualize the information in the book?

4 replies

Ron Woerner 4 days ago

Risk assessments, security assessments, and threat modeling are related, but different.

NIST defines Threat modeling as, "*A form of risk assessment that models aspects of the attack and defense sides of a logical entity, such as a piece of data, an application, a host, a system, or an environment*." https://csrc.nist.gov/glossary/term/threat_modeling

I also recommend OWASP's page on it: https://owasp.org/www-community/Threat_Modeling

> **owasp.org**
>
> **Threat Modeling | OWASP Foundation**
>
> Threat Modeling on the main website for The OWASP Foundation. OWASP is a nonprofit foundation that works to improve the security of software.

CISSP® MENTOR PROGRAM – SESSION SEVEN

QUESTIONS.

The most common questions:

C C May 5th at 7:02 AM

Good Morning ☀️ I have a question ❓

can a security assessment based on risk (low/mid/high) serve as threat modeling? Also, is it possible to get examples of a threat model, security plan and due diligence plan so we can visualize the information in the book?

4 replies

Ron Woerner 4 days ago

Risk assessments, security assessments, and threat modeling are related, but different.

NIST defines Threat modeling as, "*A form of risk assessment that models aspects of the attack and defense sides of a logical entity, such as a piece of data, an application, a host, a system, or an environment.*" https://csrc.nist.gov/glossary/term/threat_modeling

I also recommend OWASP's page on it: https://owasp.org/www-community/Threat_Modeling

> **owasp.org**
> Threat Modeling | OWASP Foundation
> Threat Modeling on the m
> OWASP is a nonprofit fou
> software.

Threat modeling works to identify, communicate, and understand threats and mitigations within the context of protecting something of value.

CISSP® MENTOR PROGRAM – SESSION SEVEN

QUESTIONS.

Amma Manso May 5th at 9:35 AM
Hi @Brandon (FRSecure) was the informal session yesterday recorded? I didn't join as I got the email saying there was no session. However, seems I may have missed a good session.

3 replies

Ron Woerner 4 days ago
Here's the link to the recording: https://youtu.be/BPVyvg44QGw
Calling something "good" is relative... 😄

YouTube | FRSecure
Session 7: 2022 FRSecure CISSP Mentor Program — Domain 4: Communication & Network Security

CISSP® MENTOR PROGRAM – SESSION FOUR

QUESTIONS.

Kim May 5th at 11:01 AM

Does anyone have a security assessment template or guide for reviewing applications and/or software they can share? I'm curious about the difference between my company's idea of a security review and the rest of the world.

2 replies

Ron Woerner 4 days ago

OWASP is the best resource for web security and testing.

See their projects page https://owasp.org/projects/ and the OWASP Web Security Testing Guide - https://owasp.org/www-project-web-security-testing-guide/

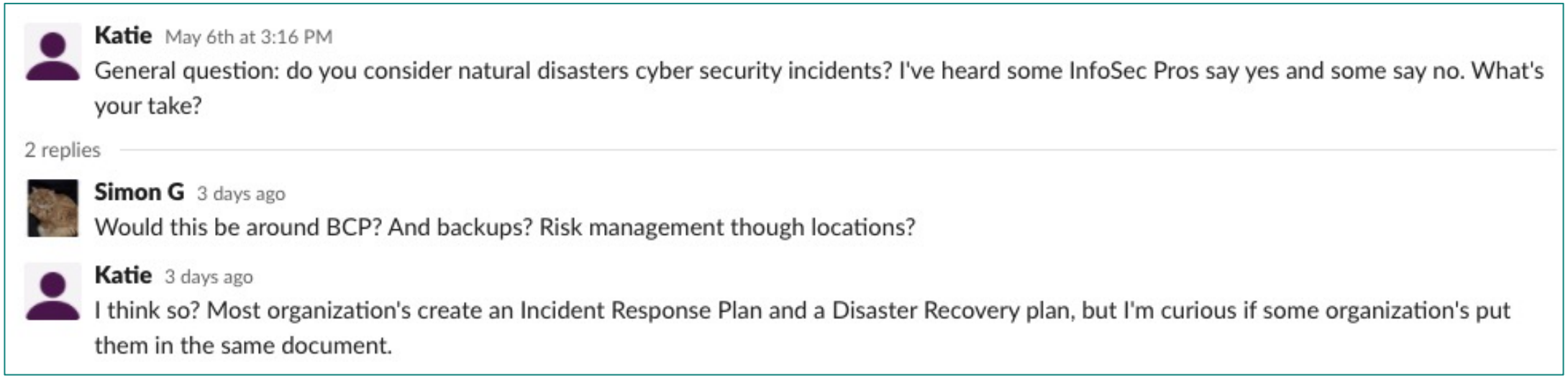
> **owasp.org**
>
> **Projects | OWASP Foundation**
>
> Projects on the main website for The OWASP Foundation. OWASP is a nonprofit foundation that works to improve the security of software.

> **owasp.org**
>
> **OWASP Web Security Testing Guide | OWASP Foundation**
>
> The Web Security Testing Guide (WSTG) Project produces the premier cybersecurity testing resource for web application developers and security professionals.

3

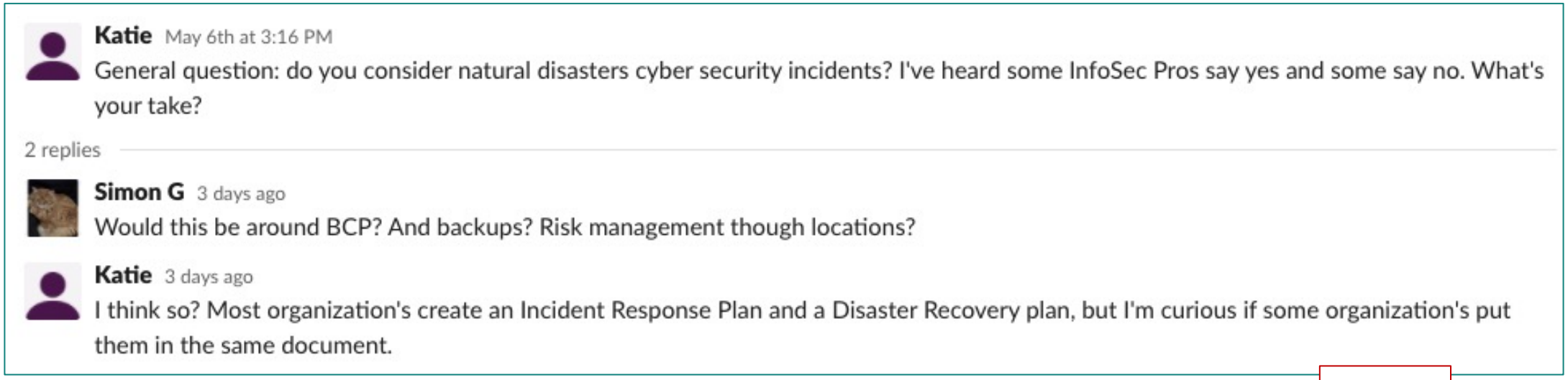
CISSP® MENTOR PROGRAM – SESSION SEVEN

QUESTIONS.



CISSP® MENTOR PROGRAM – SESSION SEVEN

QUESTIONS.



Katie May 6th at 3:16 PM
General question: do you consider natural disasters cyber security incidents? I've heard some InfoSec Pros say yes and some say no. What's your take?

2 replies

Simon G 3 days ago
Would this be around BCP? And backups? Risk management though locations?

Katie 3 days ago
I think so? Most organization's create an Incident Response Plan and a Disaster Recovery plan, but I'm curious if some organization's put them in the same document.

Threat
Natural Disaster

→

Vulnerability
Controls gap(s)

→

Incident
Bad outcome(s)

?

"Cyber"
relating to or characteristic of the culture of computers, information technology, and virtual reality.

CISSP® MENTOR PROGRAM – SESSION SEVEN

QUESTIONS.

C C May 7th at 6:37 AM
Good Morning ☀️ Question: The book mentions Typo Squatting, but did not offer any explanation on how to defend against it. Can you please provide?

4 replies

Mark Gillanders 1 day ago
what about running through opendns dot com

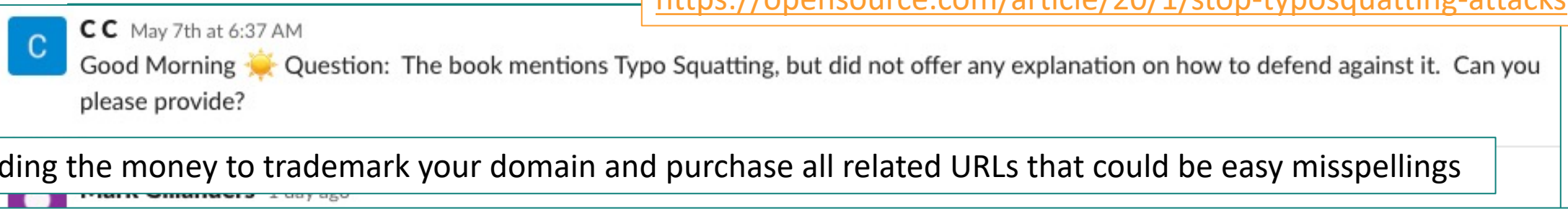
C C 1 day ago
That's a good idea. Have you used their services? Is as good as they say?

Mark Gillanders 1 day ago
Cisco since 2015

CISSP® MENTOR PROGRAM – SESSION SEVEN

QUESTIONS.

https://opensource.com/article/20/1/stop-typosquatting-attacks



spending the money to trademark your domain and purchase all related URLs that could be easy misspellings

If you need to send your users to third-party sites, do so from your official website, not in a mass email. It's important to firmly establish a policy that official communication always and only sends users to your site. That way, should a cybercriminal attempt to spoof communication from you, your users will know something's amiss when they end up on an unfamiliar page or URL structure.

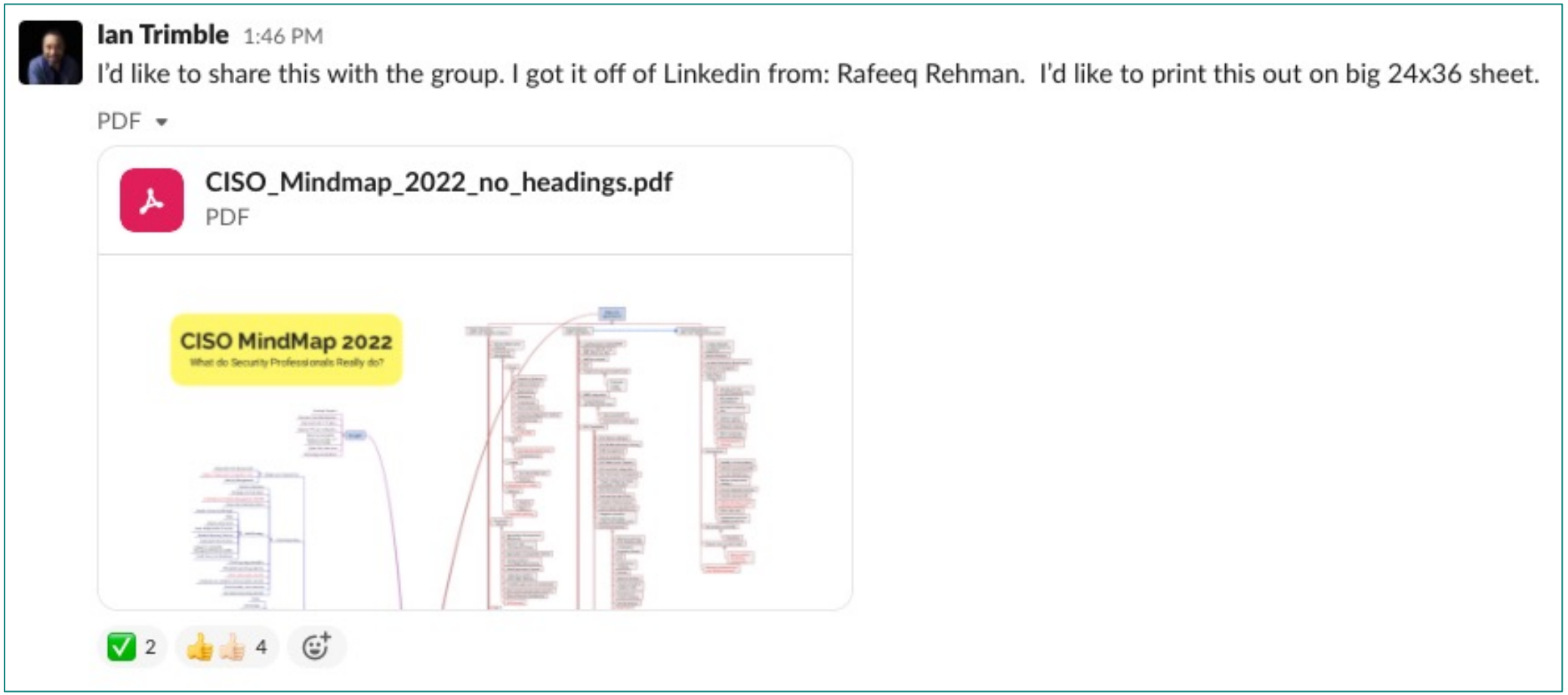
Use an open source tool like **DNS Twist** to automatically scan your company's domain and determine whether there could already be a typosquatting attack in progress. DNS Twist runs on Linux operating systems and can be used through a series of shell commands.

Some ISPs offer typosquatting protection as part of their product offering.

consider running your own DNS server along with a blacklist of incorrect and forbidden domains

CISSP® MENTOR PROGRAM – SESSION SEVEN

QUESTIONS.



CISSP® MENTOR PROGRAM – SESSION SEVEN

QUESTIONS.

C C May 7th at 2:57 PM

Questions: When performing an Administrative Investigation, at what point would you involve law enforcement ?

1 reply

Ron Woerner 14 hours ago

With investigations, I recommend you get your organization's legal department and insurance involved as early as possible. They'll be able to direct contacting law enforcement.

Law enforcement is only involved in criminal matters. Your legal team would cover any civil issues.

I hope this helps.

C C 3:29 PM

Meaning if the organization performs their own search they could lose the option for law enforcement later cause the organization performed the search on their own without warrant.

CISSP® MENTOR PROGRAM – SESSION SEVEN

QUESTIONS.

BLESSING EGEREGA Yesterday at 3:58 PM

Quick question; what layer of the OSI model does encryption occur? Encryption can happen at the presentation, session and at the network layer (i.e. IPSEC) but what's the correct answer if asked to chose one? (edited)

2 replies

Ron Woerner 8 hours ago

You are correct that encryption is at multiple layers. It's not correct to say it's only at a single layer. Defense in depth.

BLESSING EGEREGA 8 hours ago

Thanks @Ron Woerner

CISSP® MENTOR PROGRAM – SESSION SEVEN

QUESTIONS.

Rafal May 7th at 1:28 PM

Question: it's often mentioned that security controls effectiveness should be tested. I think about simple network security controls, like firewalls or proxies. How their effectiveness should be assessed? by network scans? by trying to access some resource from the network it is not supposed to reach the resource?

1 reply

Ron Woerner 1 day ago

For PCI DSS, you test network segmentation - basically if a segment can be seen from outside segments.

NIST SP800-53A is also an authoritative source on assessing controls. https://csrc.nist.gov/publications/detail/sp/800-53a/rev-5/final
Testing depends on the asset being secured and the control requirements.

> **CSRC | NIST**
>
> **NIST Special Publication (SP) 800-53A Rev. 5, Assessing Security and Privacy Controls in Information Systems and Organizations**
>
> This publication provides a methodology and set of procedures for conducting assessments of security and privacy controls employed within systems and organizations within an effective risk management framework. The assessment procedures, executed at various phases of the system development life cycle, are

INTRODUCTION

Agenda

Some testable goodies tonight!

- ~~Welcome, Reminders, & Introduction~~
- ~~Questions~~
- **Domain 4 – Communication and Network Security (pp. 334 - Kindle)**
  - Review (a little).
  - Cheat Sheet
  - **Secure Network Components**
  - **Implement Secure Communication Channels According to Design**

INTRODUCTION

Agenda

Some testable goodies tonight!

- ~~Welcome, Reminders, & Introduction~~
- ~~Questions~~
- **Domain 4 – Communication and Network Security**
  - Re
  - Ch
  - **Se**
  - **Implement Secure Communication Channels According to Design**

But we NEED a dad joke first!

CISSP® MENTOR PROGRAM – SESSION SEVEN

DAD JOKE…

If you don't like it, it's Brad's fault!

What did one Dorito farmer say to the other?

CISSP® MENTOR PROGRAM – SESSION SEVEN

DAD JOKE…

If you don't like it, it's Brad's fault!

😂😂😂

What did one Dorito farmer say to the other?

Cool Ranch!

pp. 334 - Kindle

DOMAIN 4: COMMUNICATION AND NETWORK SECURITY

Secure Network Components

An introduction to the **key concepts** associated with operating **network hardware**, followed by coverage of network **transmission media** and network components (such as firewalls, routers, and switches), ending with some foundational coverage of **endpoint security**.

DOMAIN 4: COMMUNICATION AND NETWORK SECURITY

Secure Network Components

To securely implement and use/operate network equipment, we must account for (at a minimum):

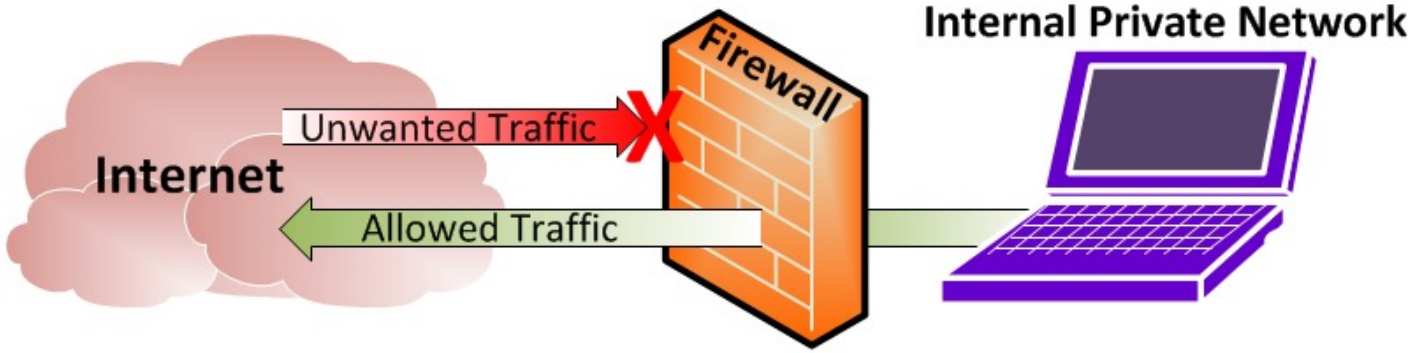
- **Policy**, **Standards**, **Guidelines**, and **Procedures**.
- Personnel must be enabled to perform; they must be **trained**.
- *We can't secure what we can't control* – **Change control** is fundamental.
- *What we can't prevent, we must be able to detect* – **Monitoring** is also fundamental.
- Other considerations include **inventory**, **redundancy**, **maintenance**, etc.

CISSP® MENTOR PROGRAM – SESSION SEVEN

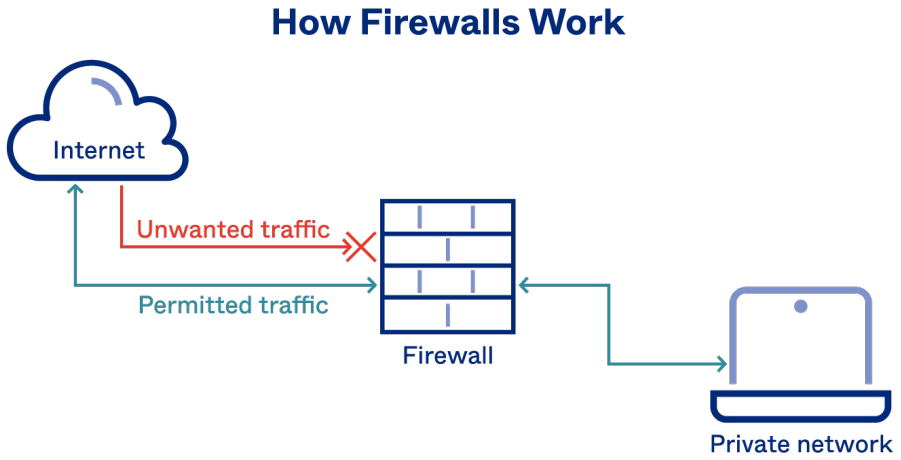
DOMAIN 4: COMMUNICATION AND NETWORK SECURITY

Secure Network Components

Firewalls



Sort of…



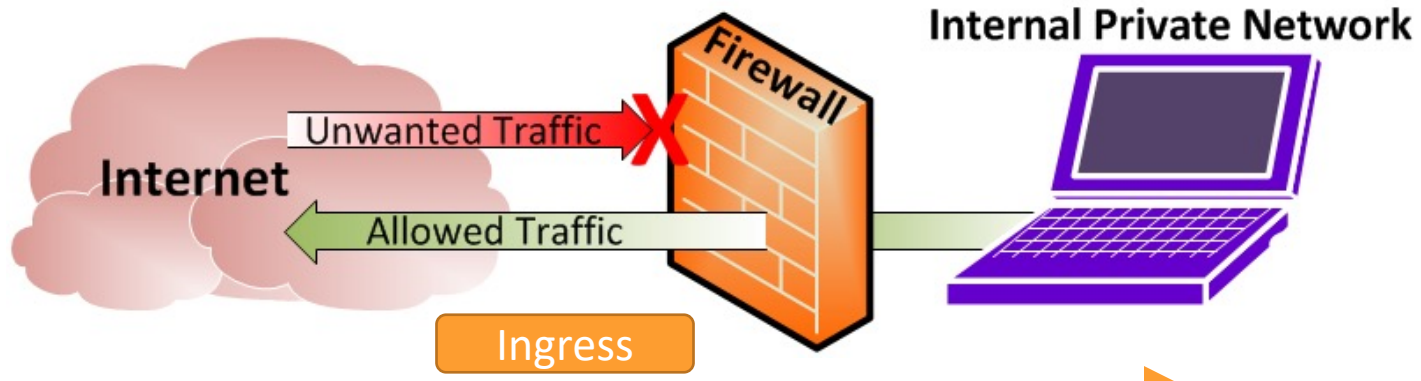
okta

CISSP® MENTOR PROGRAM – SESSION SEVEN

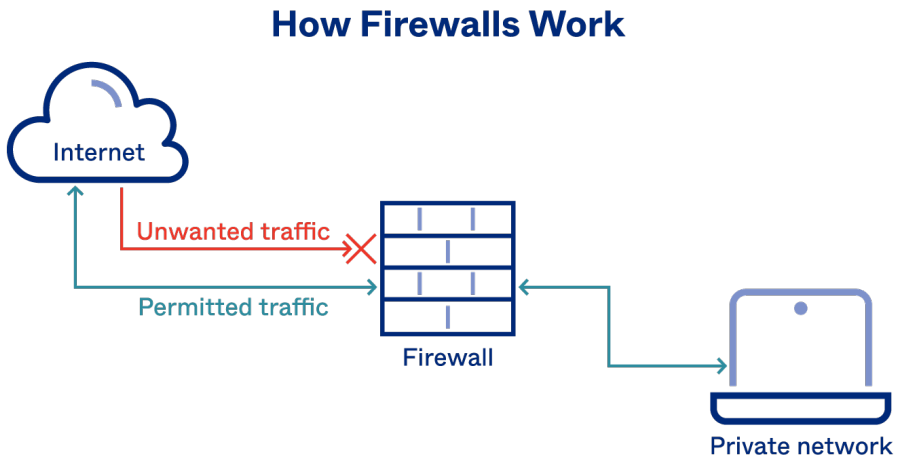
DOMAIN 4: COMMUNICATION AND NETWORK SECURITY

Secure Network Components

Firewalls



Do NOT forget



okta

DOMAIN 4: COMMUNICATION AND NETWORK SECURITY

Secure Network Components

Firewalls

- Stop unwanted (or unauthorized network traffic) based upon rules.
- Creates a “boundary”.
- Perimeter firewalls (between public/private) and internal firewalls (between various security domains).
- A “default deny” approach is most secure, but also the most work.
- Must be maintained just like any other piece of hardware running software (access control, change control, patching, etc.).
- Critical events should be logged (and monitored).

DOMAIN 4: COMMUNICATION AND NETWORK SECURITY

Secure Network Components

Firewalls – Four (basic) Types

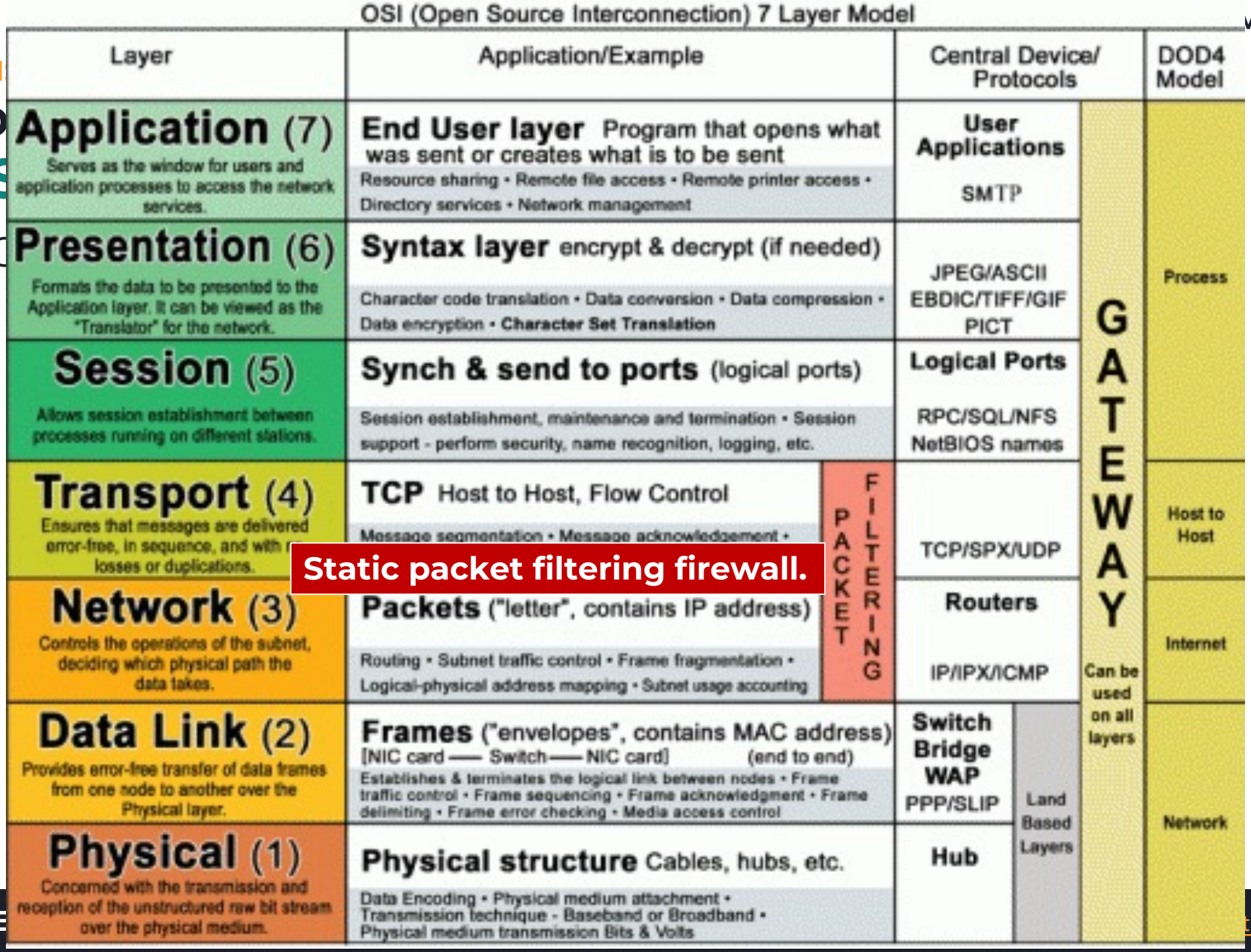
- Static packet filtering firewall.
- Application-level firewall.
- Stateful inspection firewall.
- Circuit-level firewall.

DOMAIN 4: COMMUNICATION AND NETWORK SECURITY

Secure Network Components

Firewalls – Four (basic) Types

- Static packet filtering firewall.



DOMAIN 4: COMMUNICATION AND NETWORK SECURITY

Secure Network Components

Firewalls – Four (basic) Types

- **Static packet filtering firewall.**
  - "screening router"
  - Very fast, simple, easiest to bypass/least secure.

DOMAIN 4: COMMUNICATION AND NETWORK SECURITY

Secure Network Components

Firewalls – Four (basic) Types

- **Static packet filtering firewall.**
  - "screening router"
  - Very fast, simple, easiest to bypass/least secure.
- **Application-level firewall.**

Application-level firewall.

Static packet filtering firewall.

OSI (Open Source Interconnection) 7 Layer Model

Layer	Application/Example		Central Device/ Protocols		DOD4 Model
Application (7) Serves as the window for users and application processes to access the network services.	**End User layer** Program that opens what was sent or creates what is to be sent Resource sharing • Remote file access • Remote printer access • Directory services • Network management		**User Applications** SMTP	GATEWAY	Process
Presentation (6) Formats the data to be presented to the Application layer. It can be viewed as the "Translator" for the network.	**Syntax layer** encrypt & decrypt (if needed) Character code translation • Data conversion • Data compression • Data encryption • **Character Set Translation**		JPEG/ASCII EBDIC/TIFF/GIF PICT		
Session (5) Allows session establishment between processes running on different stations.	**Synch & send to ports** (logical ports) Session establishment, maintenance and termination • Session support - perform security, name recognition, logging, etc.		**Logical Ports** RPC/SQL/NFS NetBIOS names		
Transport (4) Ensures that messages are delivered error-free, in sequence, and with [illegible] losses or duplications.	**TCP** Host to Host, Flow Control Message segmentation • Message acknowledgement •	PACKET FILTERING	TCP/SPX/UDP		Host to Host
Network (3) Controls the operations of the subnet, deciding which physical path the data takes.	**Packets** ("letter", contains IP address) Routing • Subnet traffic control • Frame fragmentation • Logical-physical address mapping • Subnet usage accounting		**Routers** IP/IPX/ICMP		Internet
Data Link (2) Provides error-free transfer of data frames from one node to another over the Physical layer.	**Frames** ("envelopes", contains MAC address) [NIC card — Switch — NIC card] (end to end) Establishes & terminates the logical link between nodes • Frame traffic control • Frame sequencing • Frame acknowledgment • Frame delimiting • Frame error checking • Media access control		**Switch Bridge WAP** PPP/SLIP	Land Based Layers	Network
Physical (1) Concerned with the transmission and reception of the unstructured raw bit stream over the physical medium.	**Physical structure** Cables, hubs, etc. Data Encoding • Physical medium attachment • Transmission technique - Baseband or Broadband • Physical medium transmission Bits & Volts		**Hub**		

GATEWAY: Can be used on all layers

DOMAIN 4: COMMUNICATION AND NETWORK SECURITY

Secure Network Components

Firewalls – Four (basic) Types

- **Static packet filtering firewall.**
  - "screening router"
  - Very fast, simple, easiest to bypass/least secure.
- **Application-level firewall.**
  - "gateway" or "proxy"
  - Slow, complex, very secure.

DOMAIN 4: COMMUNICATION AND NETWORK SECURITY

Secure Network Components

Firewalls – Four (basic) Types

- **Static packet filtering firewall.**
  - "screening router"
  - Very fast, simple, easiest to bypass/least secure.
- **Application-level firewall.**
  - "gateway" or "proxy"
  - Slow, complex, very secure.
- **Stateful inspection firewall.**

Cl

D

S

C

OSI (Open Source Interconnection) 7 Layer Model

Layer	Application/Example	Central Device/ Protocols	DOD4 Model
Application (7) Serves as the window for users and application processes to access the network services.	**End User layer** Program that opens what was sent or creates what is to be sent Resource sharing • Remote file access • Remote printer access • Directory services • Network management	**User Applications** SMTP	Process
Presentation (6) Formats the data to be presented to the Application layer. It can be viewed as the "Translator" for the network.	**Syntax layer** encrypt & decrypt (if needed) Character code translation • Data conversion • Data compression • Data encryption • **Character Set Translation**	JPEG/ASCII EBDIC/TIFF/GIF PICT	
Session (5) Allows session establishment between processes running on different stations.	**Synch & send to ports** (logical ports) Session establishment, maintenance and termination • Session support - perform security, name recognition, logging, etc.	**Logical Ports** RPC/SQL/NFS NetBIOS names	
Transport (4) Ensures that messages are delivered error-free, in sequence, and with losses or duplications.	**TCP** Host to Host, Flow Control Message segmentation • Message acknowledgement •		Host to Host
Network (3) Controls the operations of the subnet, deciding which physical path the data takes.	**Packets** ("letter", contains IP address) Routing • Subnet traffic control • Frame fragmentation • Logical-physical address mapping • Subnet usage accounting	**Routers** IP/IPX/ICMP	Internet
Data Link (2) Provides error-free transfer of data frames from one node to another over the Physical layer.	**Frames** ("envelopes", contains MAC address) [NIC card — Switch — NIC card] (end to end) Establishes & terminates the logical link between nodes • Frame traffic control • Frame sequencing • Frame acknowledgment • Frame delimiting • Frame error checking • Media access control	**Switch Bridge WAP** PPP/SLIP	Network
Physical (1) Concerned with the transmission and reception of the unstructured raw bit stream over the physical medium.	**Physical structure** Cables, hubs, etc. Data Encoding • Physical medium attachment • Transmission technique - Baseband or Broadband • Physical medium transmission Bits & Volts	**Hub**	

PACKET FILTERING

Land Based Layers

GATEWAY

Can be used on all layers

Application-level firewall.

Static packet filtering firewall.

Stateful inspection firewall.

DOMAIN 4: COMMUNICATION AND NETWORK SECURITY

Secure Network Components

Firewalls – Four (basic) Types

- **Static packet filtering firewall.**
  - "screening router"
  - Very fast, simple, easiest to bypass/least secure.
- **Application-level firewall.**
  - "gateway" or "proxy"
  - Slow, complex, very secure.
- **Stateful inspection firewall.**
  - Like a static packet filtering firewall but maintains "state".
  - Fast, harder to bypass, doesn't see data.

DOMAIN 4: COMMUNICATION AND NETWORK SECURITY

Secure Network Components

Firewalls – Four (basic) Types

- **Static packet filtering firewall.**
  - "screening router"
  - Very fast, simple, easiest to bypass/least secure.
- **Application-level firewall.**
  - "gateway" or "proxy"
  - Slow, complex, very secure.
- **Stateful inspection firewall.**
  - Like a static packet filtering firewall but maintains "state".
  - Fast, harder to bypass, doesn't see data.
- **Circuit-level firewall.**

Cl

D

S

C

OSI (Open Source Interconnection) 7 Layer Model

Layer	Application/Example	Central Device/ Protocols		DOD4 Model
Application (7) Serves as the window for users and application processes to access the network services.	**End User layer** Program that opens what was sent or creates what is to be sent Resource sharing • Remote file access • Remote printer access • Directory services • Network management	**User Applications** SMTP	GATEWAY	Process
Presentation (6) Formats the data to be presented to the Application layer. It can be viewed as the "Translator" for the network.	**Syntax layer** encrypt & decrypt (if needed) Character code translation • Data conversion • Data compression • Data encryption • **Character Set Translation**	JPEG/ASCII EBDIC/TIFF/GIF PICT		
Session (5) Allows session establishment between processes running on different stations.	**S** ical ports) Session establishment, maintenance and termination • Session support - perform security, name recognition, logging, etc.	**Logical Ports** RPC/SQL/NFS NetBIOS names		Host to Host
Transport (4) Ensures that messages are delivered error-free, in sequence, and with losses or duplications.	**TCP** Host to Host, Flow Control Message segmentation • Message acknowledgement •	PACKET FILTERING		
Network (3) Controls the operations of the subnet, deciding which physical path the data takes.	**Packets** ("letter", contains IP address) Routing • Subnet traffic control • Frame fragmentation • Logical-physical address mapping • Subnet usage accounting	**Routers** IP/IPX/ICMP	Can be used on all layers	Internet
Data Link (2) Provides error-free transfer of data frames from one node to another over the Physical layer.	**Frames** ("envelopes", contains MAC address) [NIC card — Switch — NIC card] (end to end) Establishes & terminates the logical link between nodes • Frame traffic control • Frame sequencing • Frame acknowledgment • Frame delimiting • Frame error checking • Media access control	**Switch Bridge WAP** PPP/SLIP	Land Based Layers	Network
Physical (1) Concerned with the transmission and reception of the unstructured raw bit stream over the physical medium.	**Physical structure** Cables, hubs, etc. Data Encoding • Physical medium attachment • Transmission technique - Baseband or Broadband • Physical medium transmission Bits & Volts	**Hub**		

Application-level firewall.

Circuit-level firewall.

Static packet filtering firewall.

Stateful inspection firewall.

DOMAIN 4: COMMUNICATION AND NETWORK SECURITY

Secure Network Components

Firewalls – Four (basic) Types

- **Static packet filtering firewall.**
  - "screening router"
  - Very fast, simple, easiest to bypass/least secure.
- **Application-level firewall.**
  - "gateway" or "proxy"
  - Slow, complex, very secure.
- **Stateful inspection firewall.**
  - Like a static packet filtering firewall but maintains "state".
  - Fast, harder to bypass, doesn't see data.
- **Circuit-level firewall.**
  - Operates like a stateful inspection firewall.
  - No data inspection, semi-proxy (traffic appears as though it comes from the gateway).

DOMAIN 4: COMMUNICATION AND NETWORK SECURITY

Secure Network Components

Firewalls – Four (basic) Types

- **Static packet filtering firewall.**
  - "screening router"
  - Very fast, simple, easiest to bypass/least secure.
- **Application-level firewall.**
  - "gateway" or "proxy"
  - Slow, complex, very secure.
- **Stateful inspection firewall.**
  - Like a static packet filtering firewall but maintains "state".
  - Fast, harder to bypass, doesn't see data.
- **Circuit-level firewall.**
  - Operates like a stateful inspection firewall.
  - No data inspection, semi-proxy (traffic appears as though it comes from the gateway).

Next-gen firewalls (NGFW)

- "advanced" features.
- Intrusion detection (IDS)
- Intrusion prevention (IPS)
- Can operate at all/different levels of OSI

DOMAIN 4: COMMUNICATION AND NETWORK SECURITY

Secure Network Components

Firewalls – Architectures

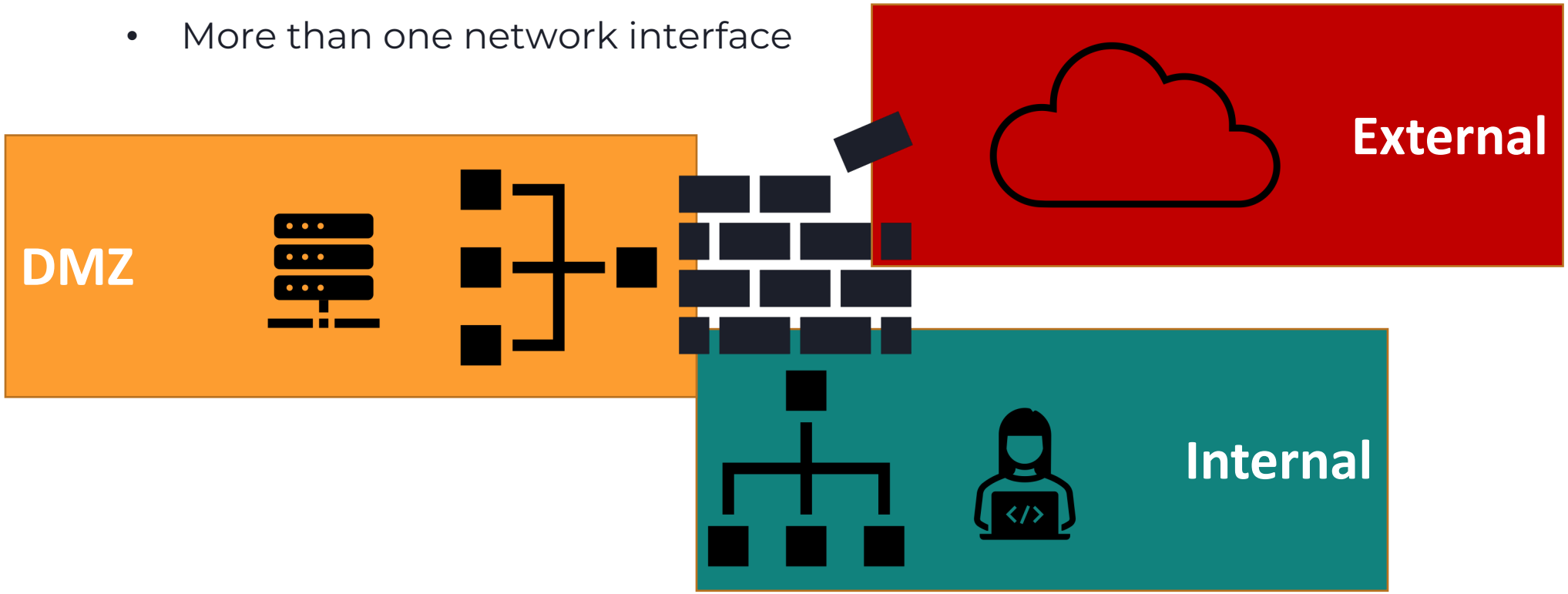
- **Multihomed Firewalls**
  - More than one network interface
- **Application-level firewall.**
  - “gateway” or “proxy”
  - Slow, complex, very secure.
- **Stateful inspection firewall.**
  - Like a static packet filtering firewall but maintains “state”.
  - Fast, harder to bypass, doesn’t see data.
- **Circuit-level firewall.**
  - Operates like a stateful inspection firewall.
  - No data inspection, semi-proxy (traffic appears as though it comes from the gateway).

DOMAIN 4: COMMUNICATION AND NETWORK SECURITY

Secure Network Components

Firewalls – Architectures

- **Multihomed Firewall**
  - More than one network interface



DOMAIN 4: COMMUNICATION AND NETWORK SECURITY

Secure Network Components

Firewalls – Architectures

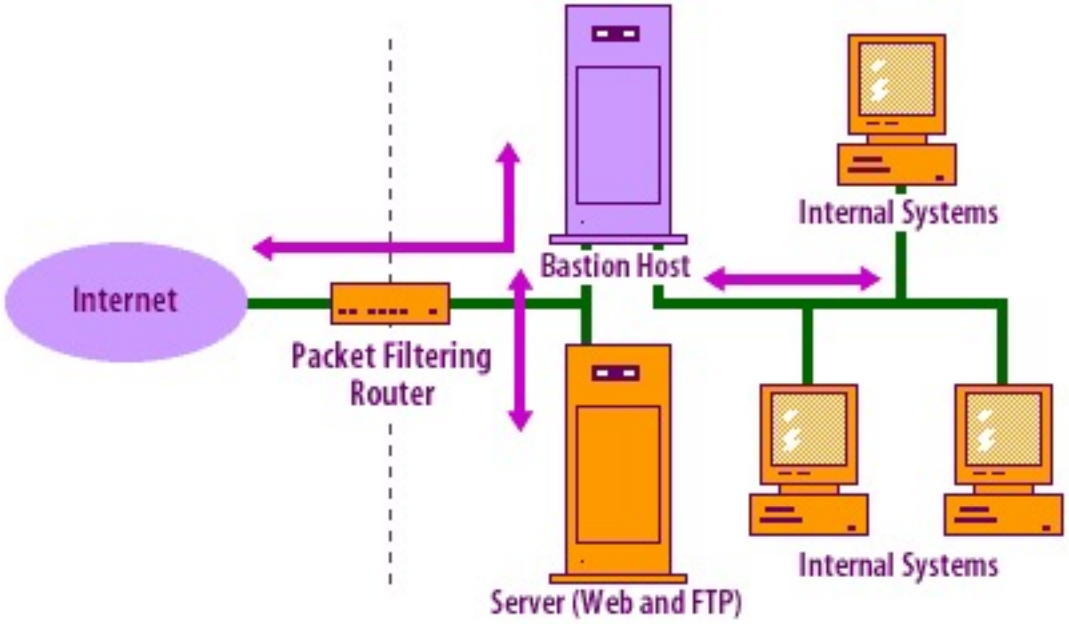
- **Multihomed Firewall**
  - More than one network interface
- **Bastion Host/Screened Host**
  - Sometimes referred to as “jump box”.
  - A proxy, limited number of applications.

DOMAIN 4: COMMUNICATION AND NETWORK SECURITY

Secure Network Components

Firewalls – Architectures

- **Multihomed Firewall**
  - More than one network interface
- **Bastion Host/Screened Host**
  - Sometimes referred to as “jump box”.
  - A proxy, limited number of applications.



DOMAIN 4: COMMUNICATION AND NETWORK SECURITY

Secure Network Components

Firewalls – Architectures

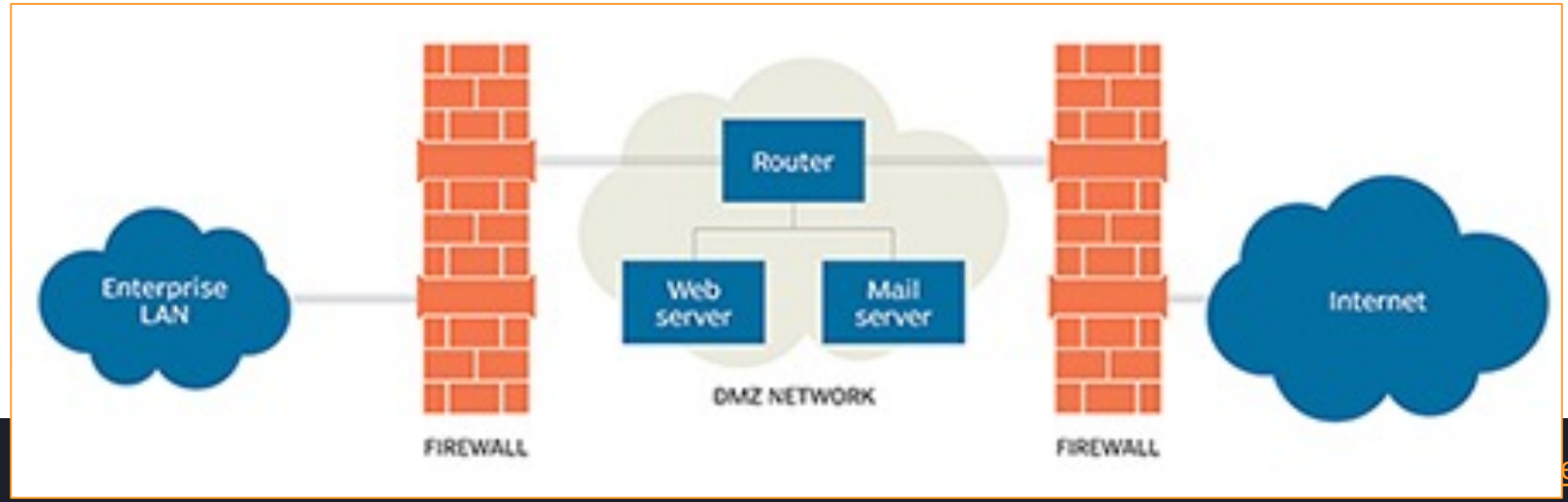
- **Multihomed Firewall**
  - More than one network interface
- **Bastion Host/Screened Host**
  - Sometimes referred to as “jump box”.
  - A proxy, limited number of applications.
- **Screened Subnet**
  - Combination of bastion hosts (but not always).

DOMAIN 4: COMMUNICATION AND NETWORK SECURITY

Secure Network Components

Firewalls – Architectures

- **Multihomed Firewall**
  - More than one network interface
- **Bastion Host/Screened Host**
  - Sometimes referred to as “jump box”.
  - A proxy, limited number of applications.
- **Screened Subnet**
  - Combination of bastion hosts (but not always).



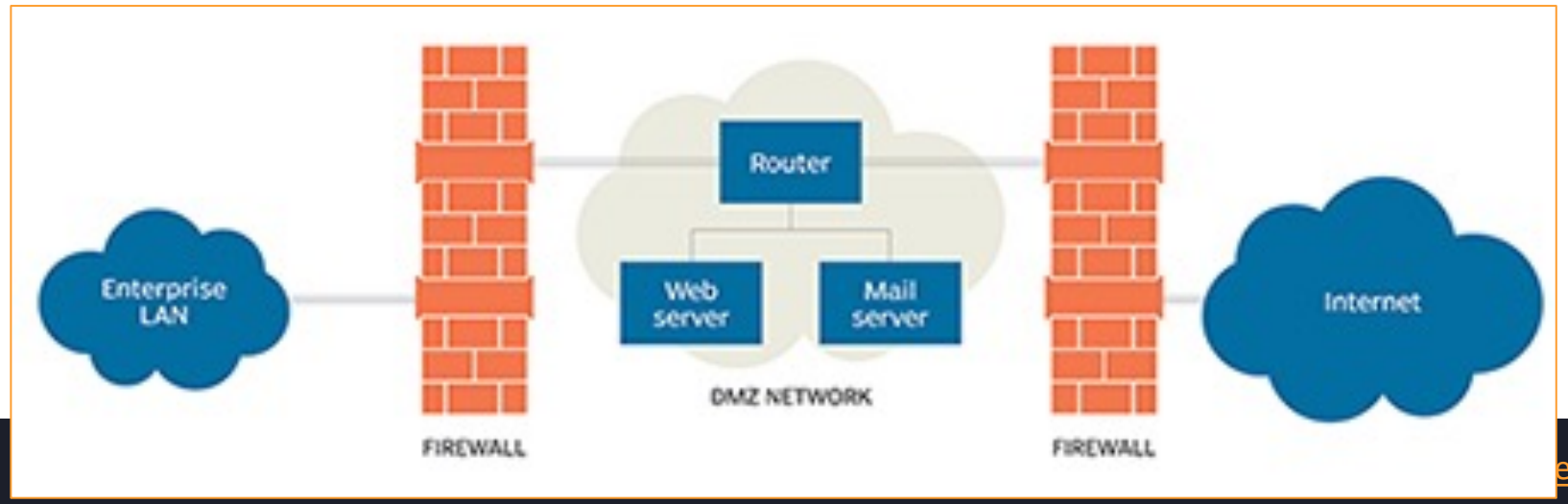
DOMAIN 4: COMMUNICATION AND NETWORK SECURITY

Secure Network Components

Firewalls – Architectures

- **Multihomed Firewall**
  - More than one network interface
- **Bastion Host/Screened Host**
  - Sometimes referred to as “jump box”.
  - A proxy, limited number of applications.
- **Screened Subnet**
  - Combination of bastion hosts (but not always).

“In today's complex computing environment, a single firewall in line between the untrusted and the private networks is almost always insufficient.”



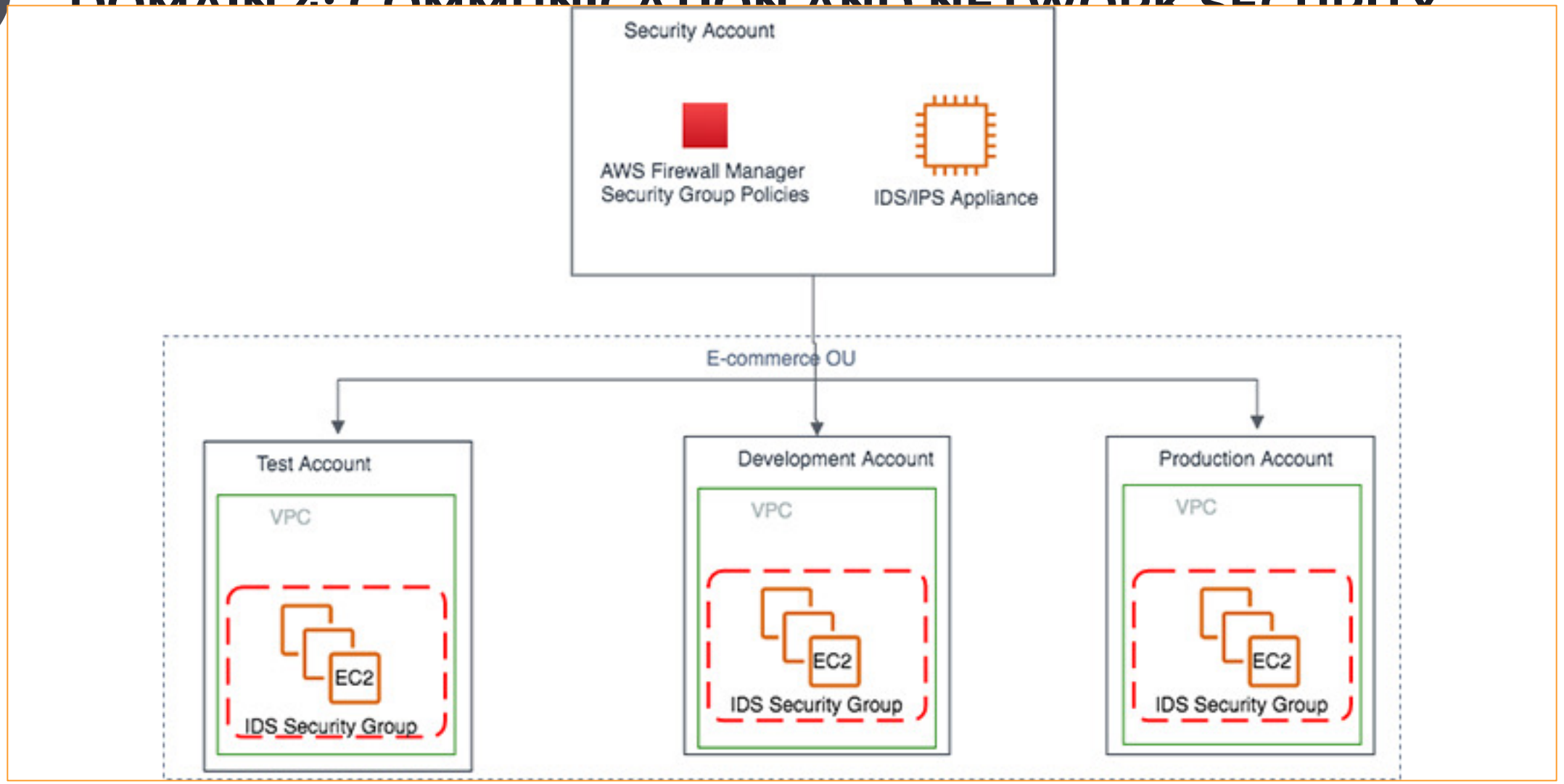
DOMAIN 4: COMMUNICATION AND NETWORK SECURITY

Secure Network Components

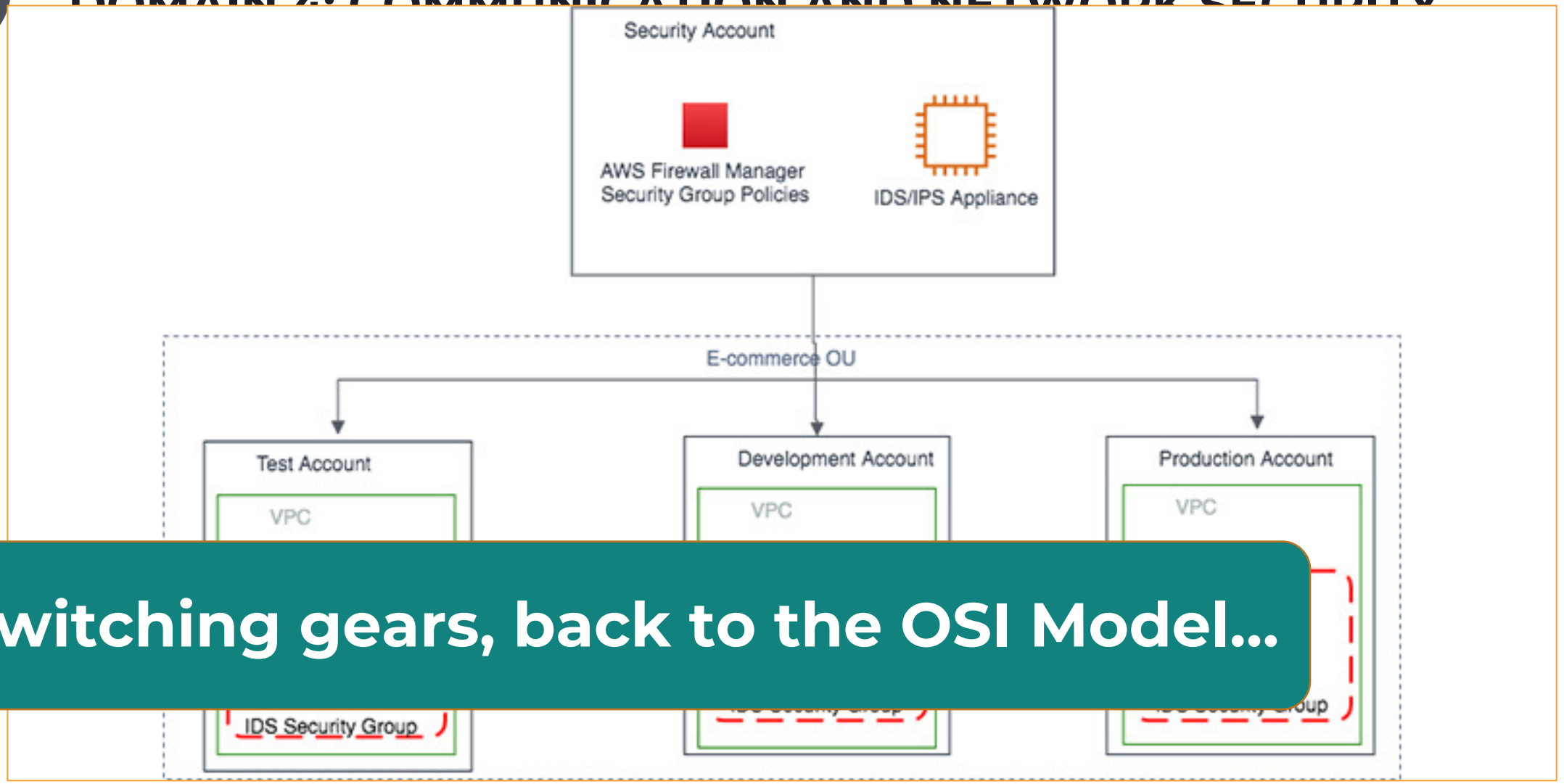
Firewalls – Architectures

- **Multihomed Firewall**
  - More than one network interface
- **Bastion Host/Screened Host**
  - Sometimes referred to as “jump box”.
  - A proxy, limited number of applications.
- **Screened Subnet**
  - Combination of bastion hosts (but not always).
- **“Other”**
  - AWS “security groups”, Virtual Private Cloud (VPC)
  - Firewall as a service (FWaaS)

DOMAIN 4: COMMUNICATION AND NETWORK SECURITY



DOMAIN 4: COMMUNICATION AND NETWORK SECURITY



Switching gears, back to the OSI Model…

Cl

D

S

C

OSI (Open Source Interconnection) 7 Layer Model

Layer	Application/Example	Central Device/ Protocols	DOD4 Model
Application (7) Serves as the window for users and application processes to access the network services.	**End User layer** Program that opens what was sent or creates what is to be sent Resource sharing • Remote file access • Remote printer access • Directory services • Network management	**User Applications** SMTP	Process
Presentation (6) Formats the data to be presented to the Application layer. It can be viewed as the "Translator" for the network.	**Syntax layer** encrypt & decrypt (if needed) Character code translation • Data conversion • Data compression • Data encryption • **Character Set Translation**	JPEG/ASCII EBDIC/TIFF/GIF PICT	
Session (5) Allows session establishment between processes running on different stations.	**S** ical ports) Session establishment, maintenance and termination • Session support - perform security, name recognition, logging, etc.	**Logical Ports** RPC/SQL/NFS NetBIOS names	
Transport (4) Ensures that messages are delivered error-free, in sequence, and with losses or duplications.	**TCP** Host to Host, Flow Control Message segmentation • Message acknowledgement •		Host to Host
Network (3) Controls the operations of the subnet, deciding which physical path the data takes.	**Packets** ("letter", contains IP address) Routing • Subnet traffic control • Frame fragmentation • Logical-physical address mapping • Subnet usage accounting	**Routers** IP/IPX/ICMP	Internet
Data Link (2) Provides error-free transfer of data frames from one node to another over the Physical layer.	**Frames** ("envelopes", contains MAC address) [NIC card — Switch — NIC card] (end to end) Establishes & terminates the logical link between nodes • Frame traffic control • Frame sequencing • Frame acknowledgment • Frame delimiting • Frame error checking • Media access control	**Switch Bridge WAP** PPP/SLIP	Network
Physical (1) Concerned with the transmission and reception of the unstructured raw bit stream over the physical medium.	**Physical structure** Cables, hubs, etc. Data Encoding • Physical medium attachment • Transmission technique - Baseband or Broadband • Physical medium transmission Bits & Volts	**Hub**	

PACKET FILTERING

GATEWAY

Can be used on all layers

Land Based Layers

Application-level firewall.

Circuit-level firewall.

Static packet filtering firewall.

Stateful inspection firewall.

Repeater and Hub

Smarter

Application-level firewall.

Circuit-level firewall.

Static packet filtering firewall.

Stateful inspection firewall.

Dumber

Repeater and Hub

OSI (Open Source Interconnection) 7 Layer Model

Layer	Application/Example	Central Device/ Protocols	DOD4 Model
Application (7) Serves as the window for users and application processes to access the network services.	**End User layer** Program that opens what was sent or creates what is to be sent Resource sharing • Remote file access • Remote printer access • Directory services • Network management	**User Applications** SMTP	Process
Presentation (6) Formats the data to be presented to the Application layer. It can be viewed as the "Translator" for the network.	**Syntax layer** encrypt & decrypt (if needed) Character code translation • Data conversion • Data compression • Data encryption • **Character Set Translation**	JPEG/ASCII EBDIC/TIFF/GIF PICT	
Session (5) Allows session establishment between processes running on different stations.	**S** gical ports) Session establishment, maintenance and termination • Session support - perform security, name recognition, logging, etc.	**Logical Ports** RPC/SQL/NFS NetBIOS names	
Transport (4) Ensures that messages are delivered error-free, in sequence, and with losses or duplications.	**TCP** Host to Host, Flow Control Message segmentation • Message acknowledgement •	PACKET FILTERING	Host to Host
Network (3) Controls the operations of the subnet, deciding which physical path the data takes.	**Packets** ("letter", contains IP address) Routing • Subnet traffic control • Frame fragmentation • Logical-physical address mapping • Subnet usage accounting	**Routers** IP/IPX/ICMP	Internet
Data Link (2) Provides error-free transfer of data frames from one node to another over the Physical layer.	**Frames** ("envelopes", contains MAC address) [NIC card — Switch — NIC card] (end to end) Establishes & terminates the logical link between nodes • Frame traffic control • Frame sequencing • Frame acknowledgment • Frame delimiting • Frame error checking • Media access control	**Switch Bridge WAP** PPP/SLIP	Network
Physical (1) Concerned with the transmission and reception of the unstructured raw bit stream over the physical medium.	**Physical structure** Cables, hubs, etc. Data Encoding • Physical medium attachment • Transmission technique - Baseband or Broadband • Physical medium transmission Bits & Volts	**Hub**	

GATEWAY — Can be used on all layers

Land Based Layers

DOMAIN 4: COMMUNICATION AND NETWORK SECURITY

Secure Network Components

Repeaters, Concentrators, and Amplifiers

- Operate at the Physical Layer (Layer 1)
- Connect two networks of the same kind together.
- Repeat/regenerate the signal (takes care of attenuation).
- Same collision domain, collision domains are segmented at Layer 2 (coming up).
- A **hub** is a multiport repeater.
- NO traffic filtering, what comes in one port goes out the other(s).
- No more than four repeaters in a row (RoT), 5-4-3 rule (5 segments, 4 repeaters, 3 have additional connections.
- **A hub is a security risk.**

N AND NETWORK SECURITY

ponents

rs, and Amplifiers

ver (Layer 1)

ne same kind together.

nal (takes care of attenuation).

- NO traffic filtering
  other(s).
- No more than fou
  segments, 4 repe
- **A hub is a securi**

Smarter

Application-level firewall.

Circuit-level firewall.

Static packet filtering firewall.

Stateful inspection firewall.

Dumber

Repeater and Hub

OSI (Open Source Interconnection) 7 Layer Model

Layer	Application/Example	Central Device/ Protocols	DOD4 Model
Application (7) Serves as the window for users and application processes to access the network services.	**End User layer** Program that opens what was sent or creates what is to be sent Resource sharing • Remote file access • Remote printer access • Directory services • Network management	**User Applications** SMTP	Process
Presentation (6) Formats the data to be presented to the Application layer. It can be viewed as the "Translator" for the network.	**Syntax layer** encrypt & decrypt (if needed) Character code translation • Data conversion • Data compression • Data encryption • **Character Set Translation**	JPEG/ASCII EBDIC/TIFF/GIF PICT	
Session (5) Allows session establishment between processes running on different stations.	**S** …gical ports) Session establishment, maintenance and termination • Session support - perform security, name recognition, logging, etc.	**Logical Ports** RPC/SQL/NFS NetBIOS names	
Transport (4) Ensures that messages are delivered error-free, in sequence, and with … losses or duplications.	**TCP** Host to Host, Flow Control Message segmentation • Message acknowledgement •		Host to Host
Network (3) Controls the operations of the subnet, deciding which physical path the data takes.	**Packets** ("letter", contains IP address) Routing • Subnet traffic control • Frame fragmentation • Logical-physical address mapping • Subnet usage accounting	**Routers** IP/IPX/ICMP	Internet
Data Link (2) Provides error-free transfer of data frames from one node to another over the Physical layer.	**Frames** ("envelopes", contains MAC address) [NIC card — Switch — NIC card] (end to end) Establishes & terminates the logical link between nodes • Frame traffic control • Frame sequencing • Frame acknowledgment • Frame delimiting • Frame error checking • Media access control	**Switch Bridge WAP** PPP/SLIP	Network
Physical (1) Concerned with the transmission and reception of the unstructured raw bit stream over the physical medium.	**Physical structure** Cables, hubs, etc. Data Encoding • Physical medium attachment • Transmission technique - Baseband or Broadband • Physical medium transmission Bits & Volts	**Hub**	

PACKET FILTERING

GATEWAY

Can be used on all layers

Land Based Layers

Smarter

Application-level firewall.

Circuit-level firewall.

Static packet filtering firewall.

Stateful inspection firewall.

Bridge and Switch

Repeater and Hub

Dumber

OSI (Open Source Interconnection) 7 Layer Model

Layer	Application/Example	Central Device/ Protocols	DOD4 Model
Application (7) Serves as the window for users and application processes to access the network services.	**End User layer** Program that opens what was sent or creates what is to be sent. Resource sharing • Remote file access • Remote printer access • Directory services • Network management	**User Applications** SMTP	Process
Presentation (6) Formats the data to be presented to the Application layer. It can be viewed as the "Translator" for the network.	**Syntax layer** encrypt & decrypt (if needed). Character code translation • Data conversion • Data compression • Data encryption • **Character Set Translation**	JPEG/ASCII EBDIC/TIFF/GIF PICT	
Session (5) Allows session establishment between processes running on different stations.	**S** …gical ports). Session establishment, maintenance and termination • Session support - perform security, name recognition, logging, etc.	**Logical Ports** RPC/SQL/NFS NetBIOS names	
Transport (4) Ensures that messages are delivered error-free, in sequence, and with … losses or duplications.	**TCP** Host to Host, Flow Control. Message segmentation • Message acknowledgement •		Host to Host
Network (3) Controls the operations of the subnet, deciding which physical path the data takes.	**Packets** ("letter", contains IP address). Routing • Subnet traffic control • Frame fragmentation • Logical-physical address mapping • Subnet usage accounting	**Routers** IP/IPX/ICMP	Internet
Data Link (2) Provides error-free transfer of data frames from one node to another over the Physical layer.	**Frames** ("envelopes", cont… [NIC card — Switch — NIC card] Establishes & terminates the logical link be… traffic control • Frame sequencing • Frame … delimiting • Frame error checking • Media …	**Switch**	Network
Physical (1) Concerned with the transmission and reception of the unstructured raw bit stream over the physical medium.	**Physical structure** Cat… Data Encoding • Physical medium attach… Transmission technique - Baseband or B… Physical medium transmission Bits & Vol…		

PACKET FILTERING

GATEWAY — Can be used on all layers

Land Based Layers

DOMAIN 4: COMMUNICATION AND NETWORK SECURITY

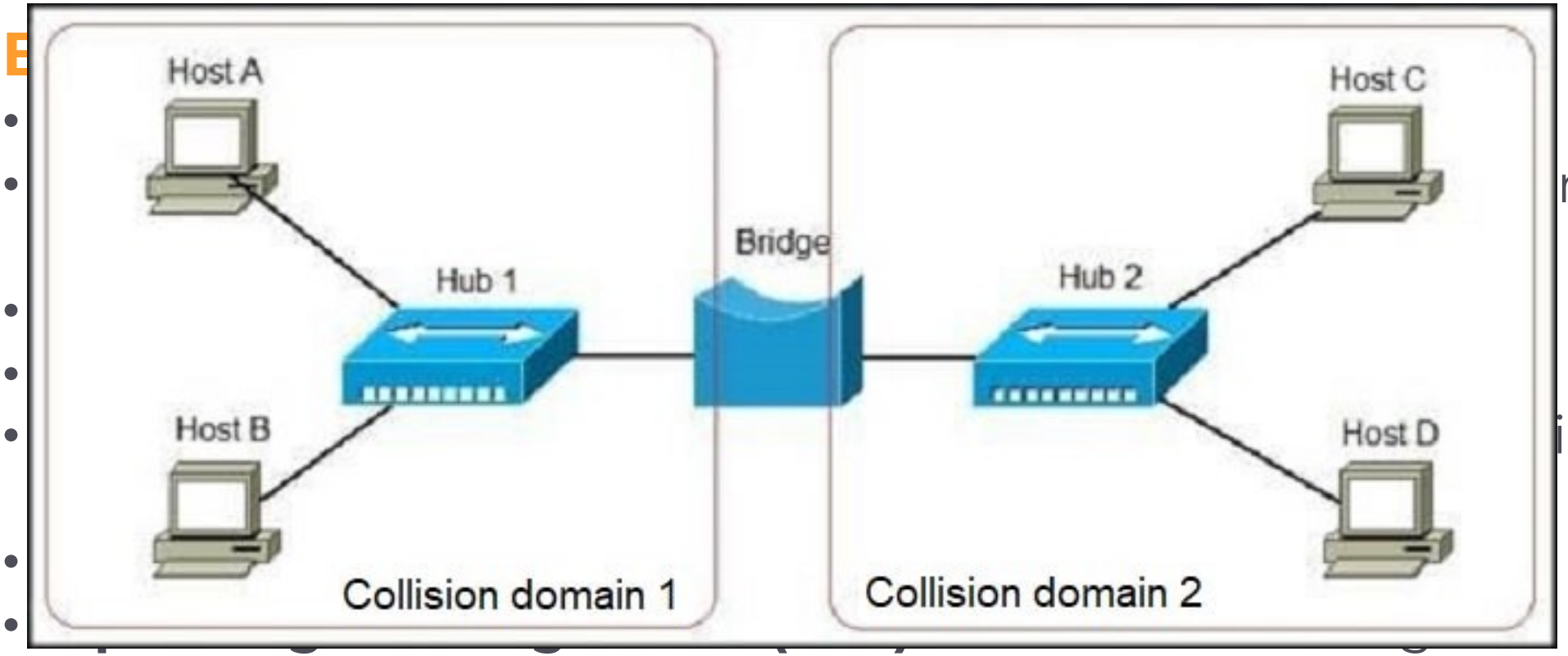
Secure Network Components

Bridges and Switches

- Operate at the Data Link Layer (Layer 2)
- Connect two networks of the same **protocol** together, can connect different physical types & speeds.
- Repeat/regenerate the signal (takes care of attenuation).
- Filters traffic based on MAC address (aka physical address).
- Breaks the collision domain, but broadcast domain remains (Layer 3).
- A **switch** is a multiport bridge.
- **Spanning Tree Algorithm (STA)** - blocks forwarding on redundant links by setting up one preferred link between switches in the LAN.

DOMAIN 4: COMMUNICATION AND NETWORK SECURITY

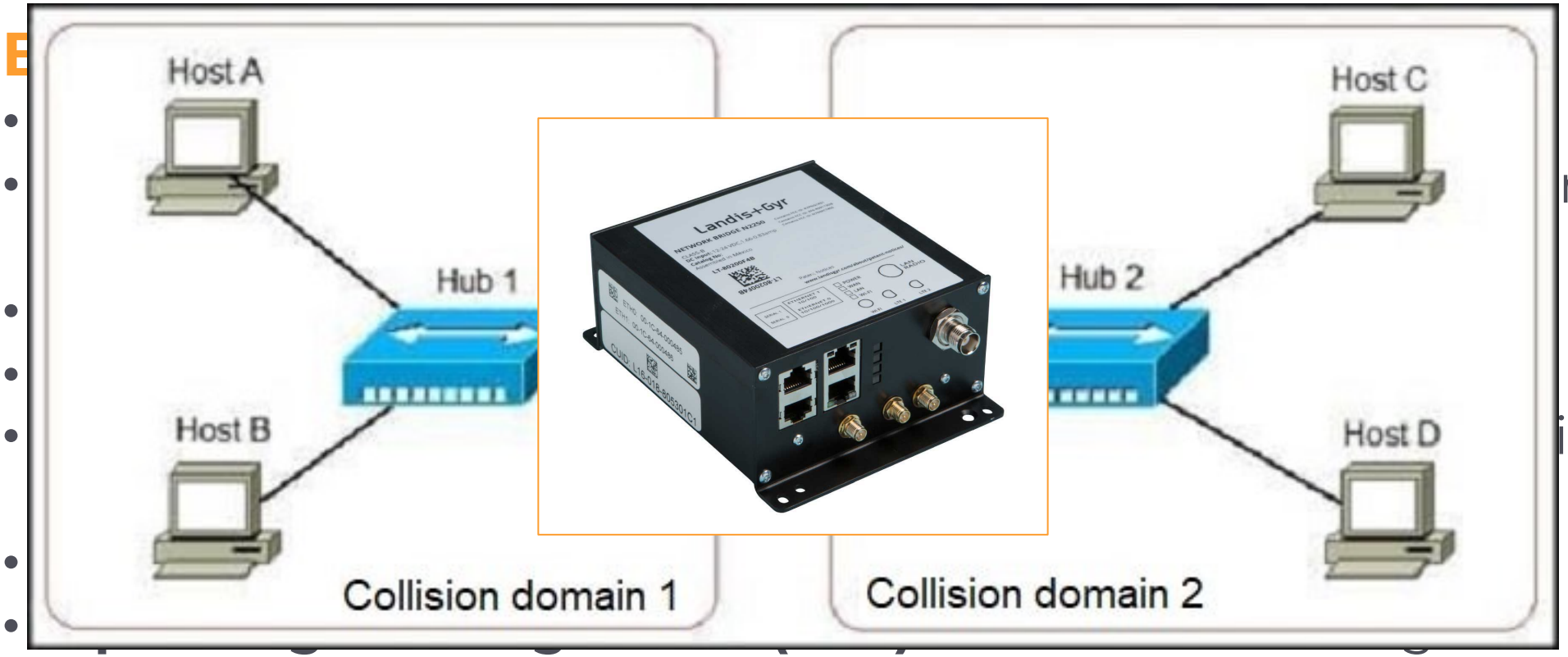
Secure Network Components



- n
- ins
- redundant links by setting up one preferred link between switches in the LAN.

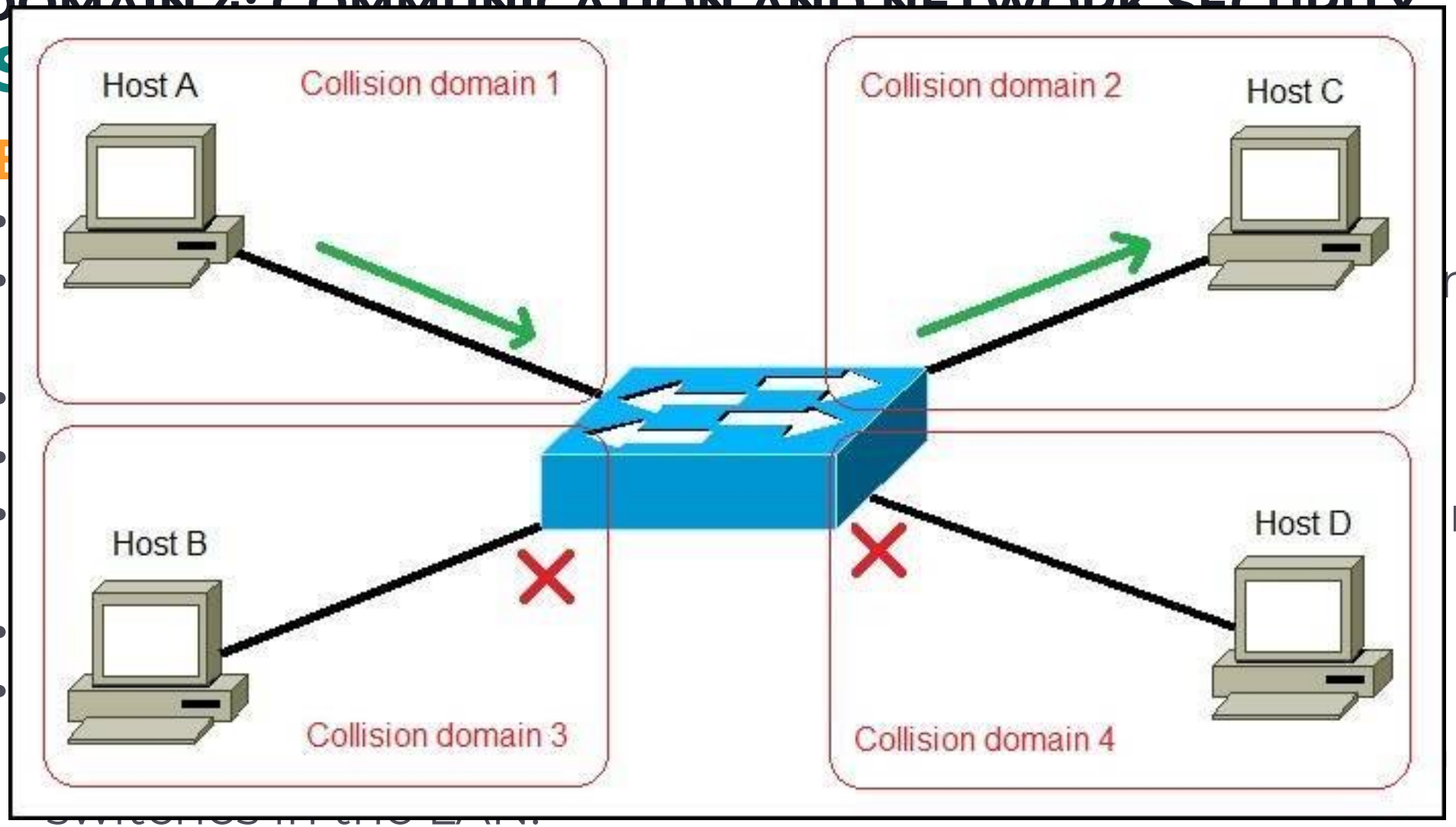
DOMAIN 4: COMMUNICATION AND NETWORK SECURITY

Secure Network Components

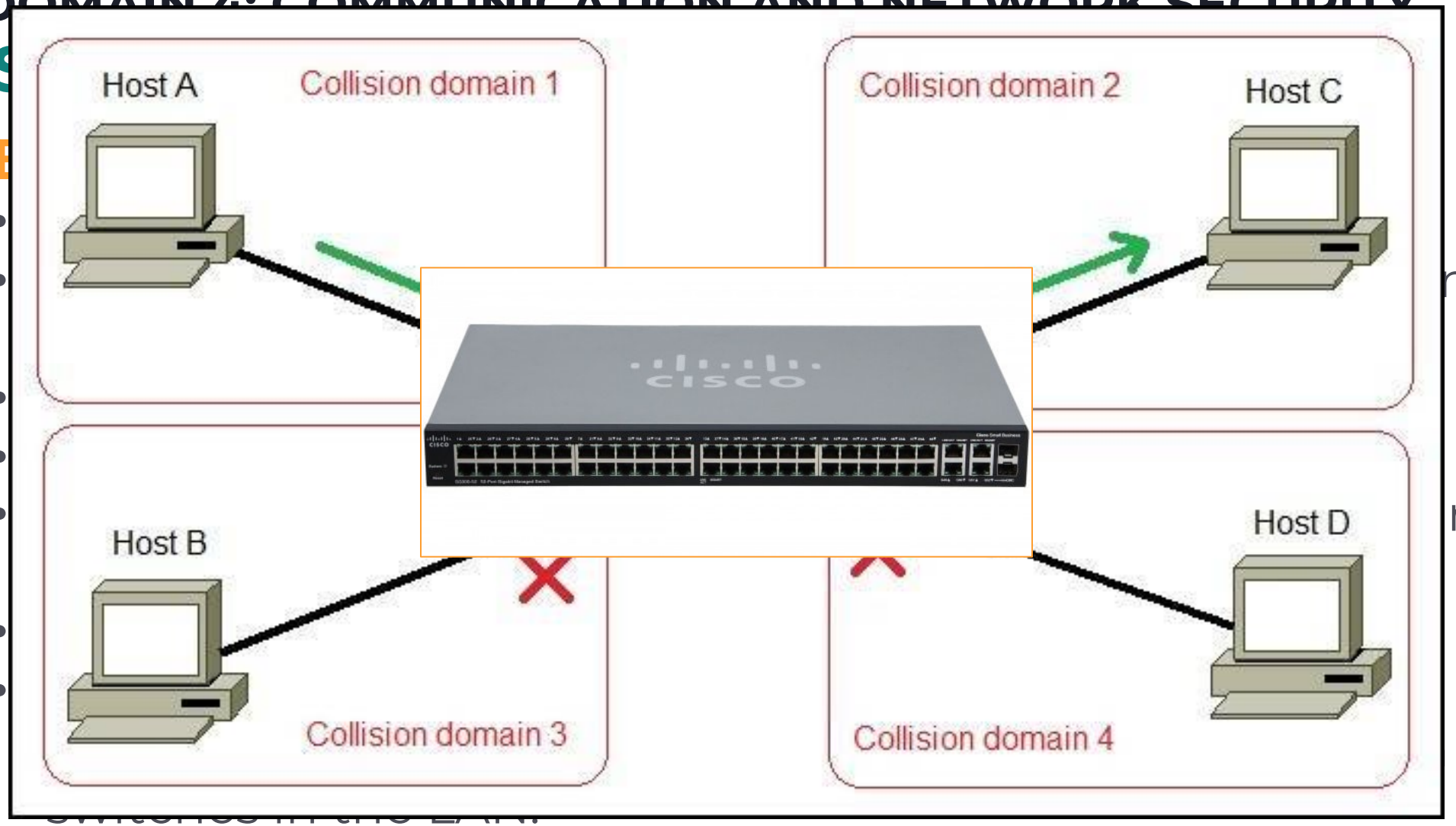


- n
- ins
- redundant links by setting up one preferred link between switches in the LAN.

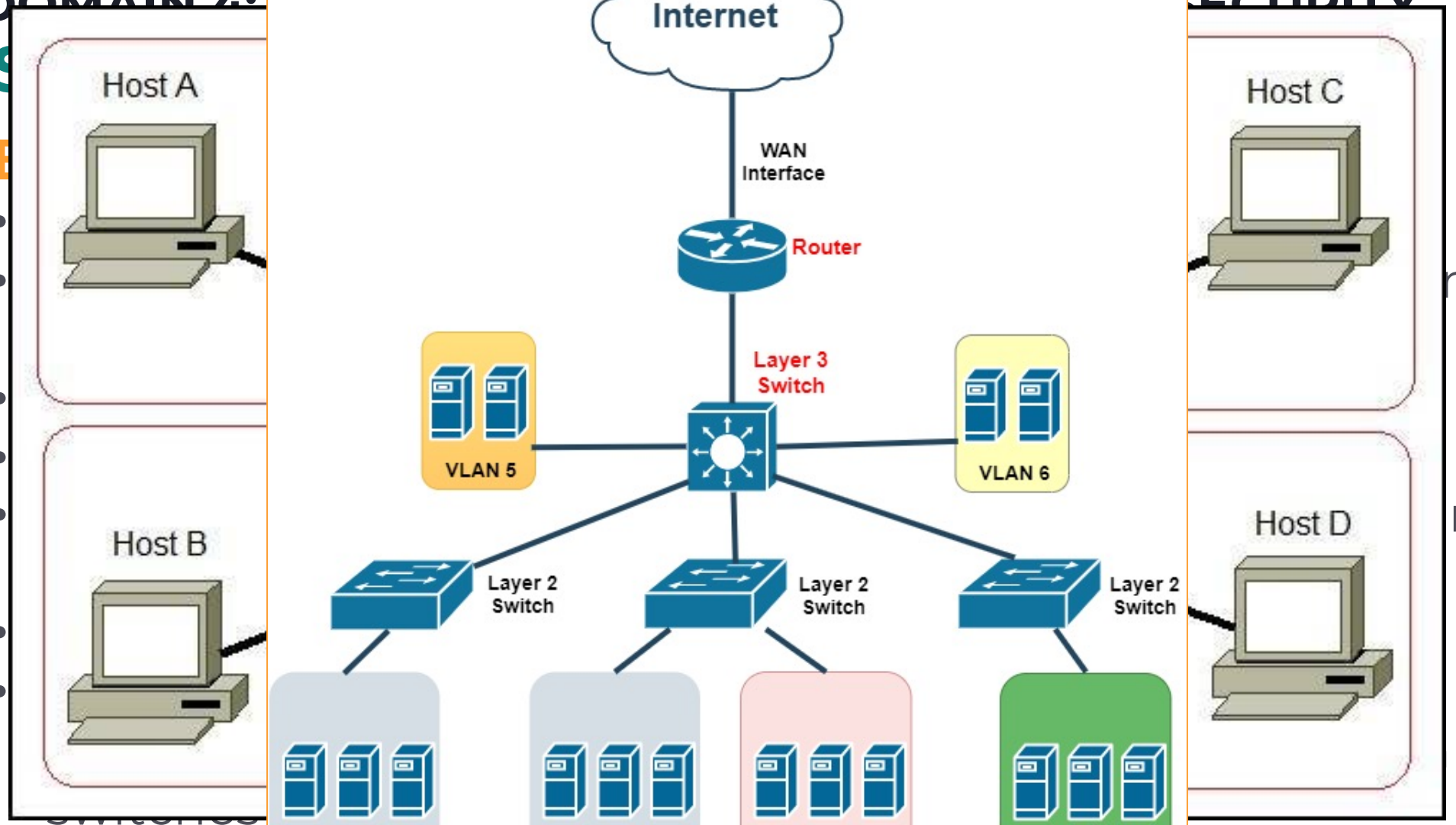
DOMAIN 4: COMMUNICATION AND NETWORK SECURITY



DOMAIN 4: COMMUNICATION AND NETWORK SECURITY



DOMAIN 4:



DOMAIN 4: COMMUNICATION AND NETWORK SECURITY

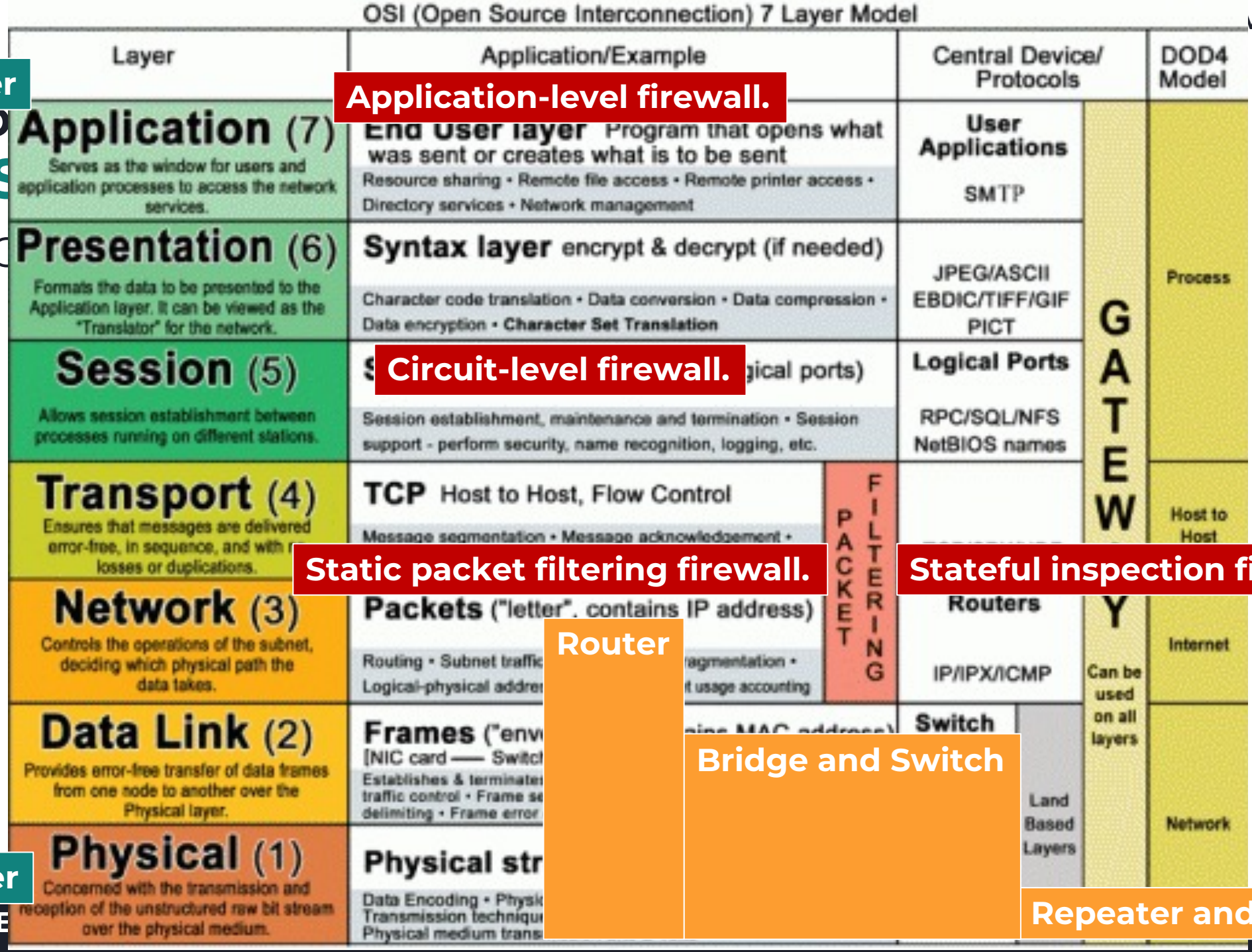
Secure Network Components

Switches

- Operate a Layer 2 and there are NO ROUTING capabilities.
- Switches can segment networks using VLANs but cannot route between VLANs without a router.
- VLANs are created by “tagging” ports in the switch.

Smarter

Dumber



Application-level firewall.

Circuit-level firewall.

Static packet filtering firewall.

Stateful inspection firewall.

Router

Bridge and Switch

Repeater and Hub

DOMAIN 4: COMMUNICATION AND NETWORK SECURITY

Secure Network Components

Routers

- Operate at the Network Layer (Layer 3)
- Connect two networks of the same **protocol** together, can connect different physical types, speeds, and layer 2 technologies (Ethernet, Token Ring, etc.).
- Repeat/regenerate the signal (takes care of attenuation).
- Filters traffic based on **IP address** (aka logical address).
- Breaks the collision domain and the **broadcast domain**.
- Determines the best route (path) through a network.
- Routing table built manually or with a routing protocol (BGP, OSPF, IGRP, EIGRP, RIP, etc.)

CIS

DC

S

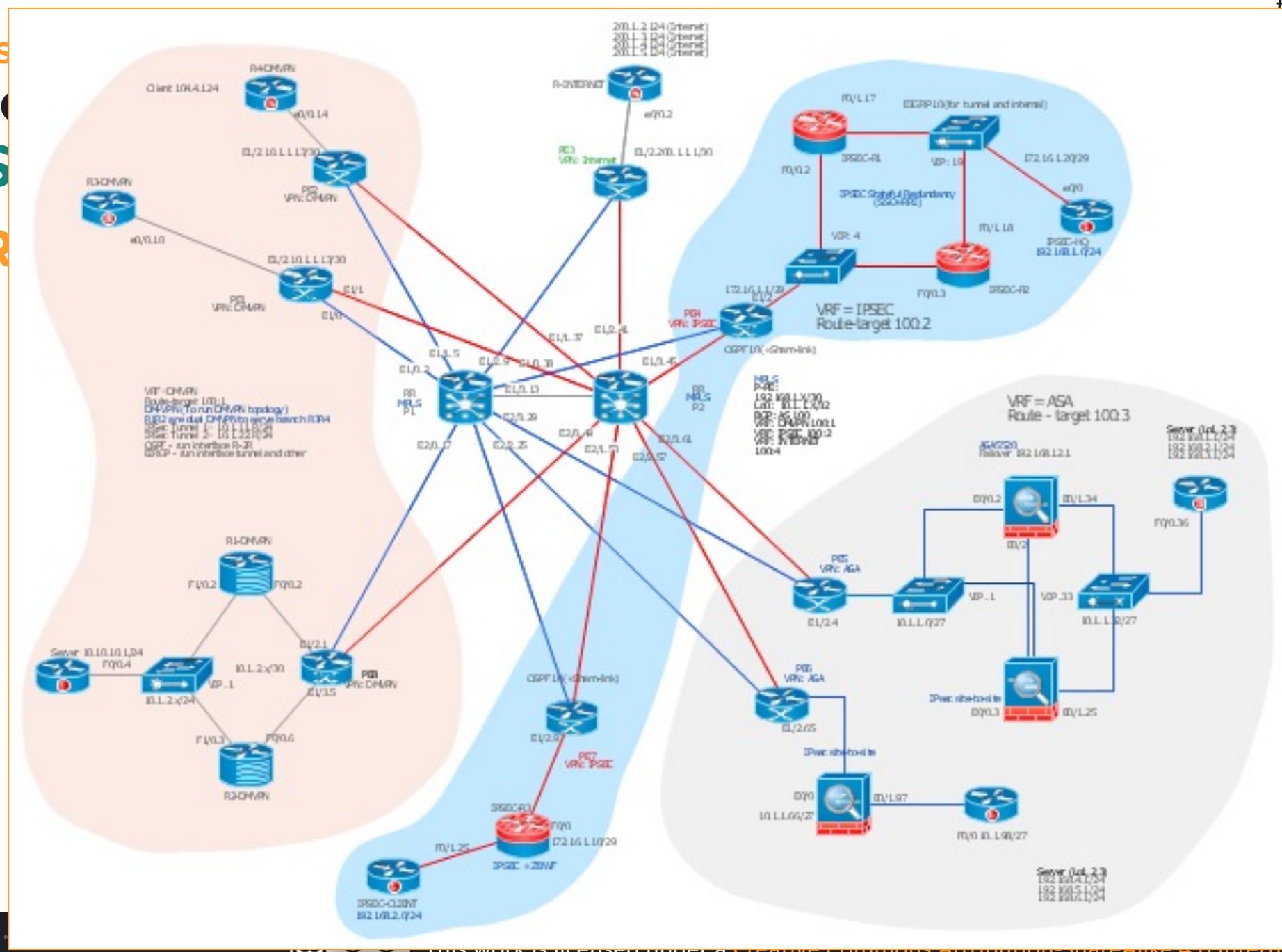
R

-
-

an

-
-
-
-
-

BGP,



Smarter

Dumber

Application-level firewall.

Gateway

Circuit-level firewall.

Static packet filtering firewall.

Stateful inspection firewall.

Router

Bridge and Switch

Repeater and Hub

OSI (Open Source Interconnection) 7 Layer Model

Layer	Application/Example	Central Device/ Protocols	DOD4 Model
App (7)	End User layer Program that opens what was sent or creates what is to be sent Resource sharing • Remote file access • Remote printer access • Directory services • Network management	User Applications SMTP	Process
Pres (6)	Syntax layer encrypt & decrypt (if needed) Character code translation • Data conversion • Data compression • Data encryption • Character Set Translation	JPEG/ASCII EBDIC/TIFF/GIF PICT	
Se	Session establishment, maintenance and termination • Session support - perform security, name recognition, logging, etc.	Logical Ports RPC/SQL/NFS NetBIOS names	
Tra (4)	TCP Host to Host, Flow Control Message segmentation • Message acknowledgement •		Host to Host
Ne	Packets ("letter", contains IP address) Routing • Subnet traffic • Logical-physical addre	Routers IP/IPX/ICMP	Internet
Dat (2)	Frames ("env [NIC card — Switch Establishes & terminate traffic control • Frame se delimiting • Frame error	Switch	Network
Ph	Physical str Data Encoding • Physi Transmission techniqu Physical medium trans		

PACKET FILTERING

GATEWAY

Can be used on all layers

Land Based Layers

DOMAIN 4: COMMUNICATION AND NETWORK SECURITY

Secure Network Components

Gateways

- Can operate at all Layers (1 – 7).
- Connect two networks of different **protocols** together.
- Also called “protocol translators”.
- Repeat/regenerate the signal (takes care of attenuation).
- Many types, including data, mail, application, internet, etc.
- Breaks the collision domain and the broadcast domain.

DOMAIN 4: COMMUNICATION AND NETWORK SECURITY

Secure Network Components

Proxies

- A type of gateway.
- Can operate at all Layers (1 – 7).
- Proxies **DO NOT** translate protocols.
- Acts on behalf of a host/hosts.
- Network Address Translation (NAT) server.
- Breaks the collision domain and the broadcast domain.

SOCKS, which stands for Socket Secure, is a network protocol that facilitates communication with servers through a firewall by routing network traffic to the actual server on behalf of a client. SOCKS is designed to route any type of traffic generated by any protocol or program.

SOCKS is a **layer 5 protocol**

DOMAIN 4: COMMUNICATION AND NETWORK SECURITY

Secure Network Components

LAN Extender

- Also called a “network extender” or “Ethernet extender.
- Any device used to extend an Ethernet or network segment beyond its inherent distance limitation which is approximately 100 meters (328 ft).
- Work at Layer 2, like a Layer 2 repeater.

Wireless Access Points

- Operate a Layer 2.
- Discussed last week in more detail.

DOMAIN 4: COMMUNICATION AND NETWORK SECURITY

Transmission Media

Local Area Network Technologies - Ethernet

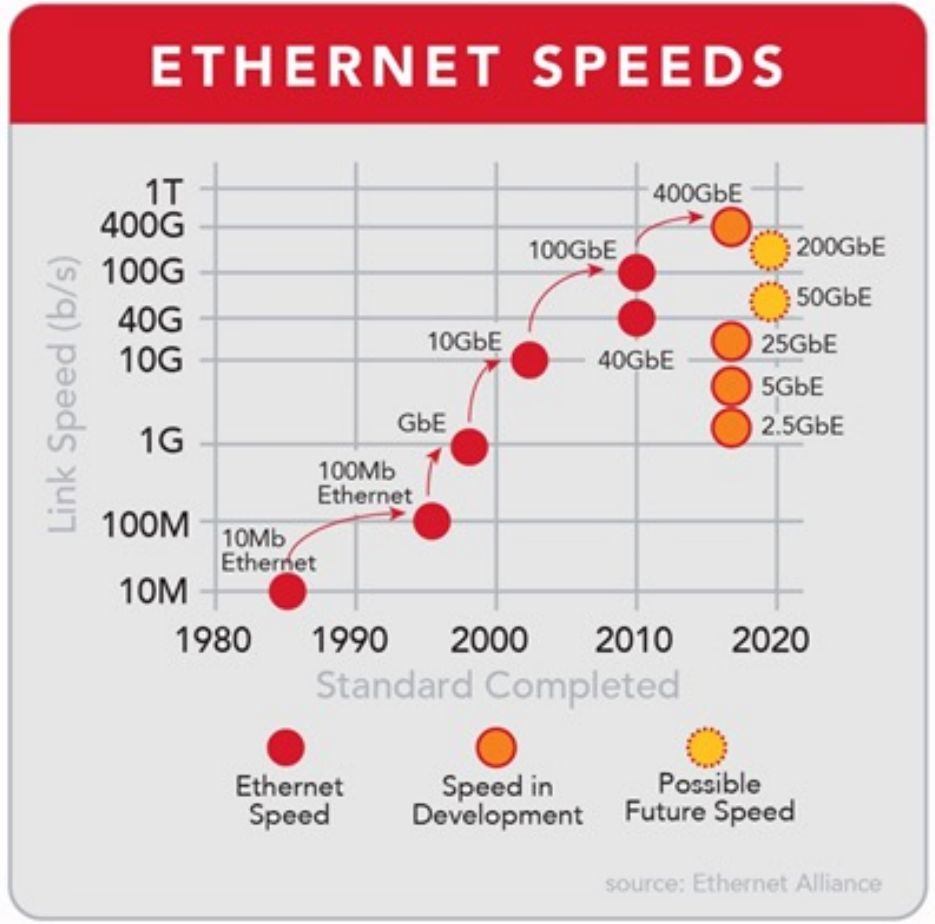
- IEEE 802.3
- Most common LAN technology in use.
- Usually, a Star or Bus topology.
- Two-way, full-duplex communication.
- Ethernet is a Layer 2 technology, also works down (at Layer 1).
- The PDU for Ethernet is a “Frame”.
- Carrier Sense Multiple Access – Collision Detect (CSMA-CD).

DOMAIN 4: COMMUNICATION AND NETWORK SECURITY

Transmission Media

Local Area Network Technologies - Ethernet

- **Fast Ethernet** – data transfer up to 100 Mbps.
- **Gigabit Ethernet** – data transfer up to 1,000 Mbps (~1 Gbps)
- **10 Gigabit Ethernet** – data transfer up to 10 Gbps (~10,000 Mbps).



DOMAIN 4: COMMUNICATION AND NETWORK SECURITY

Transmission Media

Wireless Local Area Network Technologies – Wi-Fi

- IEEE 802.11
- Two modes of operation (mostly):
  - Infrastructure Mode – client/server, clients connect to Wireless Access Points (WAPs).
  - Ad hoc Mode – Peer-to-peer connections.
- No physical media, transmission over radio waves.
- Carrier Sense Multiple Access – Collision Avoidance (CSMA-CA).

DOMAIN 4: COMMUNICATION AND NETWORK SECURITY

Transmission Media

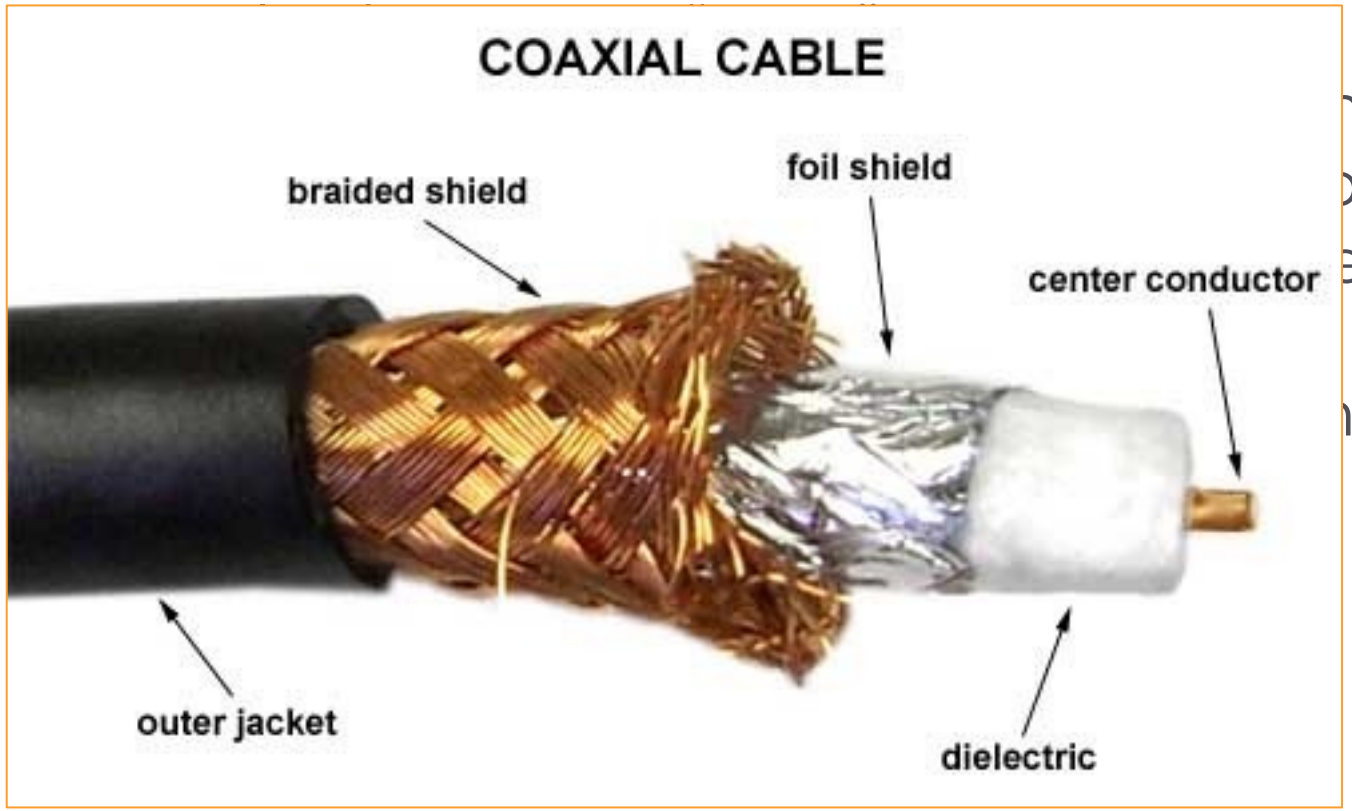
Network Cabling – Coaxial Cable

- Also known as “coax”.
- Center core of copper wire as an inner conductor surrounded by an insulating layer, surrounded by a conducting shield
- Two-way communication; the center copper core and the braided shielding layer.
- Well resistant to electromagnetic interference (EMI) and less susceptible to leakage
- Longer distance than twisted pair.

DOMAIN 4: COMMUNICATION AND NETWORK SECURITY

Transmission Media

Network Cabling – Coaxial Cable



ner conductor surrounded
by a conducting shield
er copper core and the

nterference (EMI) and less

CISSP® MENTOR PROGRAM – SESSION SEVEN

DOMAIN 4: COMMUNICATION AND NETWORK SECURITY

Tr... Ne...

Type	Impedance (ohms)	Core (mm)	Dielectric				Outside diameter		Shields	Remarks	Max. attenuation, 750 MHz (dB/100 ft)
			Type	(VF)	(in)	(mm)	(in)	(mm)			
RG-6/U	75	1.024	PF	0.75	0.185	4.7	0.270	6.86	Double	Low loss at high frequency for cable television, satellite television and cable modems	5.650
RG-6/UQ	75	1.024	PF	0.75	0.185	4.7	0.298	7.57	Quad	This is "quad shield RG-6". It has four layers of shielding; regular RG-6 has only one or two	5.650[21]
RG-7	75	1.30	PF		0.225	5.72	0.320	8.13	Double	Low loss at high frequency for cable television, satellite television and cable modems	4.570
RG-8/U	50	2.17	PE		0.285	7.2	0.405	10.3		Amateur radio; Thicknet (10BASE5) is similar	5.967[22]
RG-8X	50	1.47	PF	0.82	0.155	3.9	0.242	6.1	Single	A thinner version, with some of the electrical characteristics of RG-8U in a diameter similar to RG-59.[23]	10.946[22]
RG-9/U	51		PE				0.420	10.7			
RG-11/U	75	1.63	PE	0.66-0.85	0.285	7.2	0.412	10.5	Dual/triple/quad	Low loss at high frequency for cable and satellite television. Used for long drops and underground conduit, similar to RG7 but generally lower loss.[24][25]	3.650
RG-56/U	48	1.4859					0.308	7.82	Dual braid shielded	Rated to 8000 volts, rubber dielectric	

DOMAIN 4: COMMUNICATION AND NETWORK SECURITY

Transmission Media

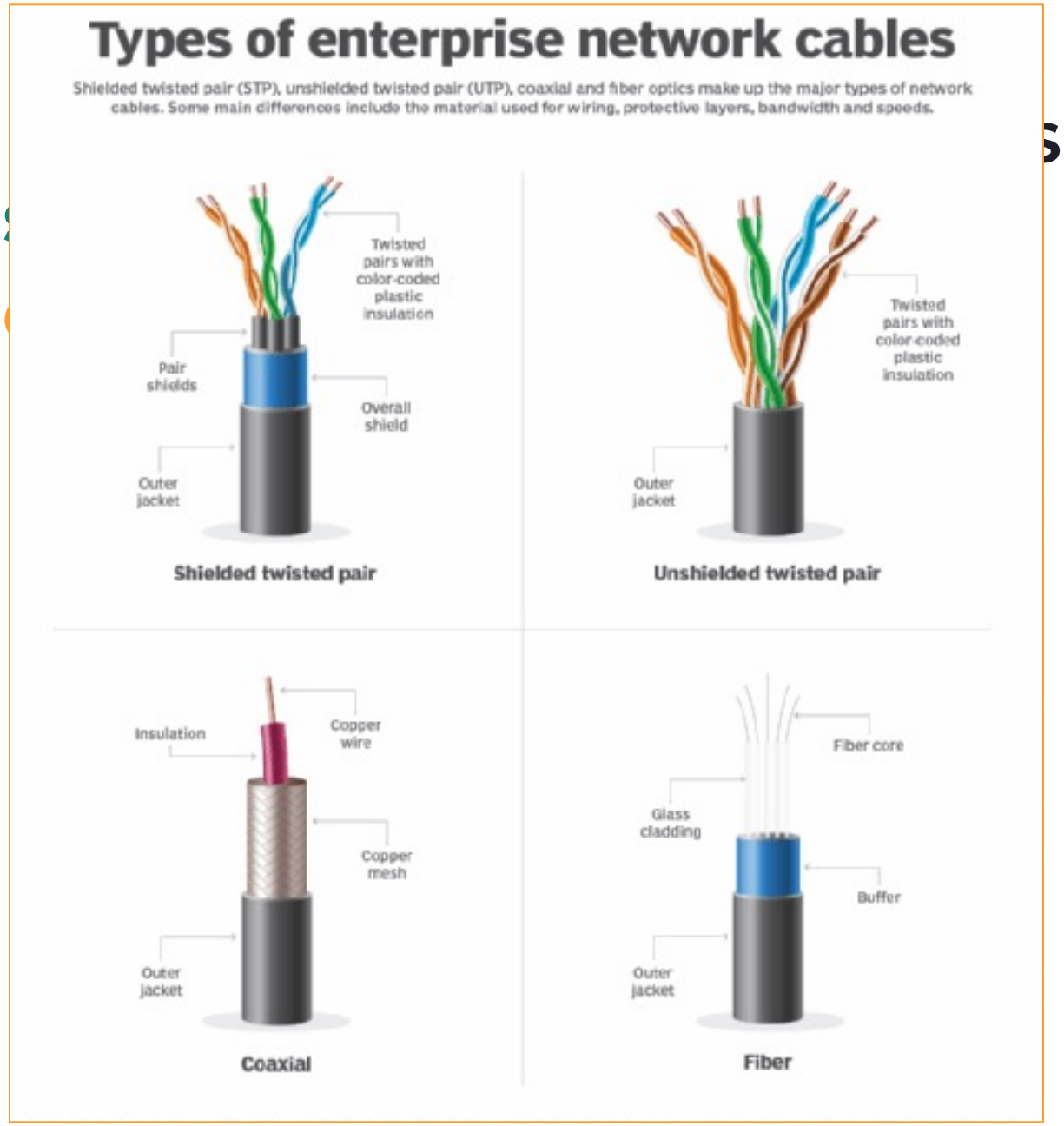
Network Cabling – Twisted Pair

CISSP® MENTOR

DOMAIN 4: ...SECURITY

Transmi...

Network ...



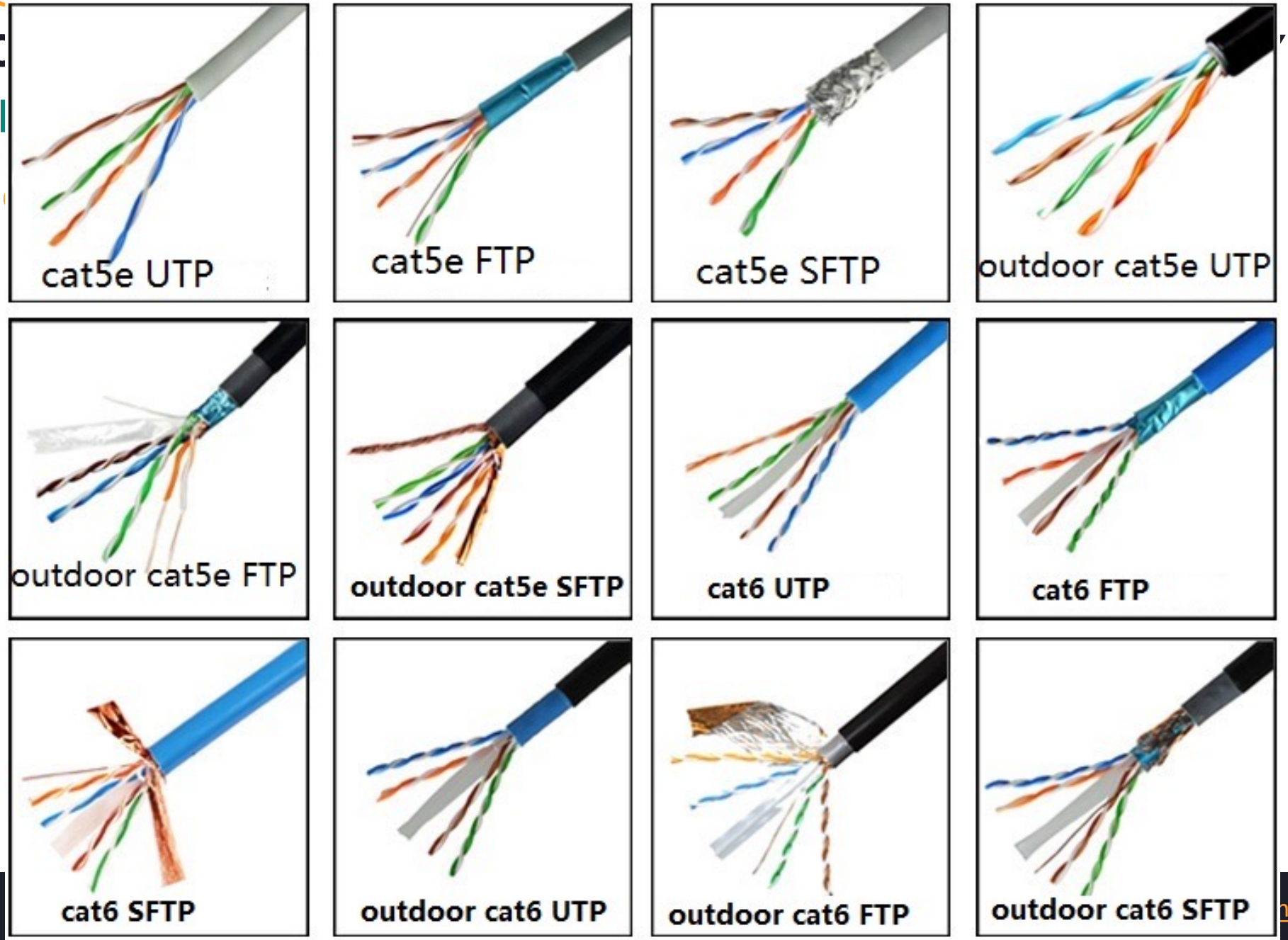
CISS

DC

T

N

Shenzhen Owire Lan Cable Manufacturer



Ethernet Cables

Ethernet Name	Cable Type	Maximum Speed	Maximum Transmission Distance	Cable Name
100Base-TX	UTP	100Mbps	100 Meters	CAT5, CAT5e, CAT6
1000Base-T	UTP	1000Mbps	100 Meters	CAT5e, CAT6
1000Base-SX	Fiber	1000Mbps	550 Meters	Multimode and Singlemode Fiber
1000Base-LX	Fiber	1000Mbps	550 Mbps MMF, 2000 Meters SMF	Singlemode Fiber
1000Base-ZX	Fiber	1000Mbps	70000 Meters (70 Kilometers)	Singlemode Fiber
10GBase-T	UTP	10Gbps	100 Meters	CAT5e, CAT6
10GBase-SR	Fiber	10Gbps	300 Meters	Multimode Fiber
10GBase-LR	Fiber	10Gbps	10000 Meters (10 Kilometers)	Singlemode Fiber
10GBase-ER	Fiber	10Gbps	40000 Meters (40 Kilometers)	Singlemode Fiber
10GBase-SW	Fiber	10Gbps	300 Meters	Multimode Fiber
10GBase-LW	Fiber	10Gbps	10000 Meters (10 Kilometers)	Singlemode Fiber
10GBase-EW	Fiber	10Gbps	40000 Meters (40 Kilometers)	Singlemode Fiber

Multimode Fiber

Singlemode Fiber

10G Multimode Fiber

SFP+Copper (Twinax)

DOMAIN 4: COMMUNICATION AND NETWORK SECURITY

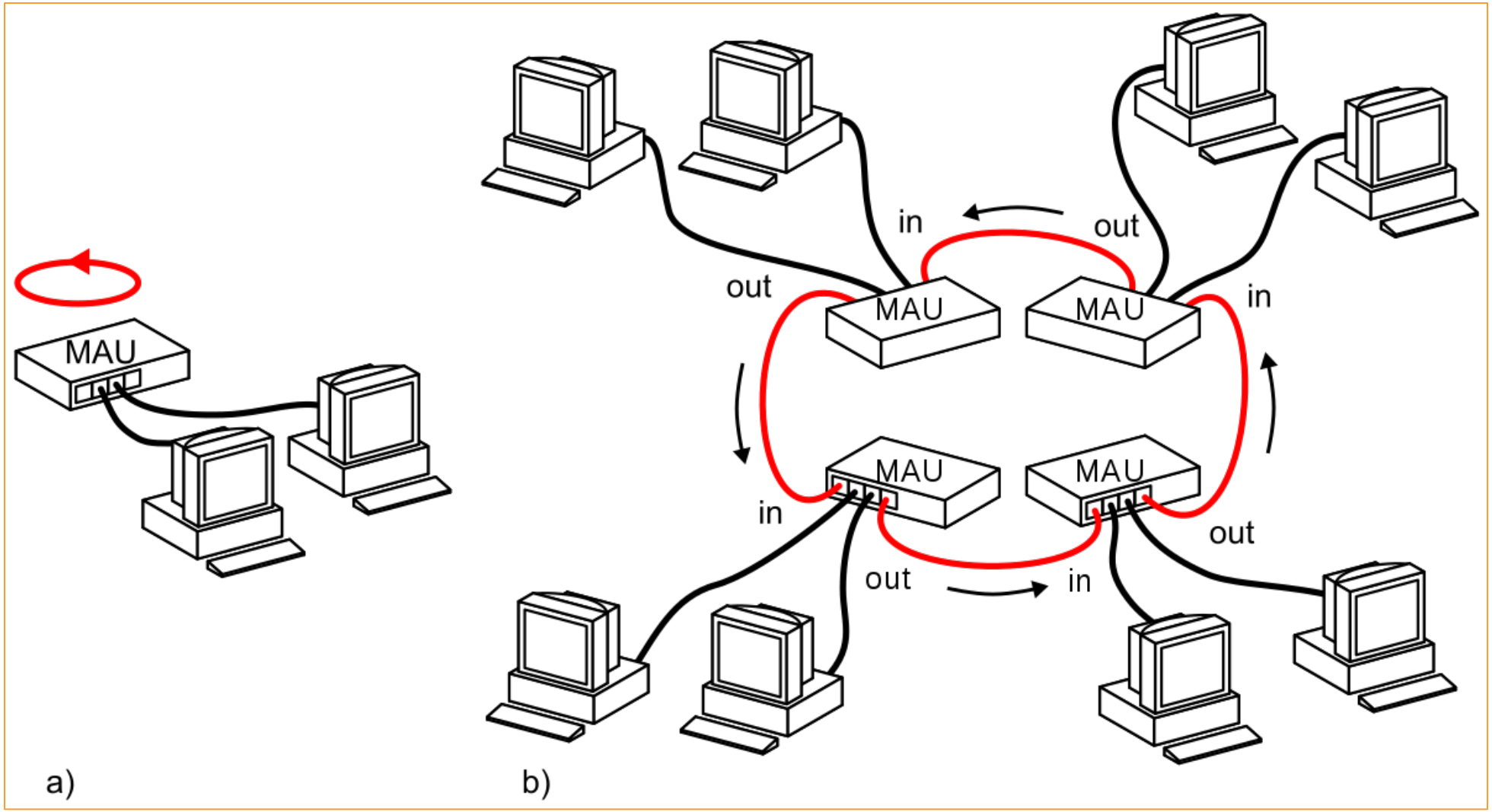
Transmission Media

Network Topologies - Ring

- A physical star, logical ring.
- No data collisions.
- Token-passing is the most common technology.
- Token Ring (IEEE 802.5)

CISSP® MENTOR PROGRAM – SESSION SEVEN

DOMAIN 4: COMMUNICATION AND NETWORK SECURITY

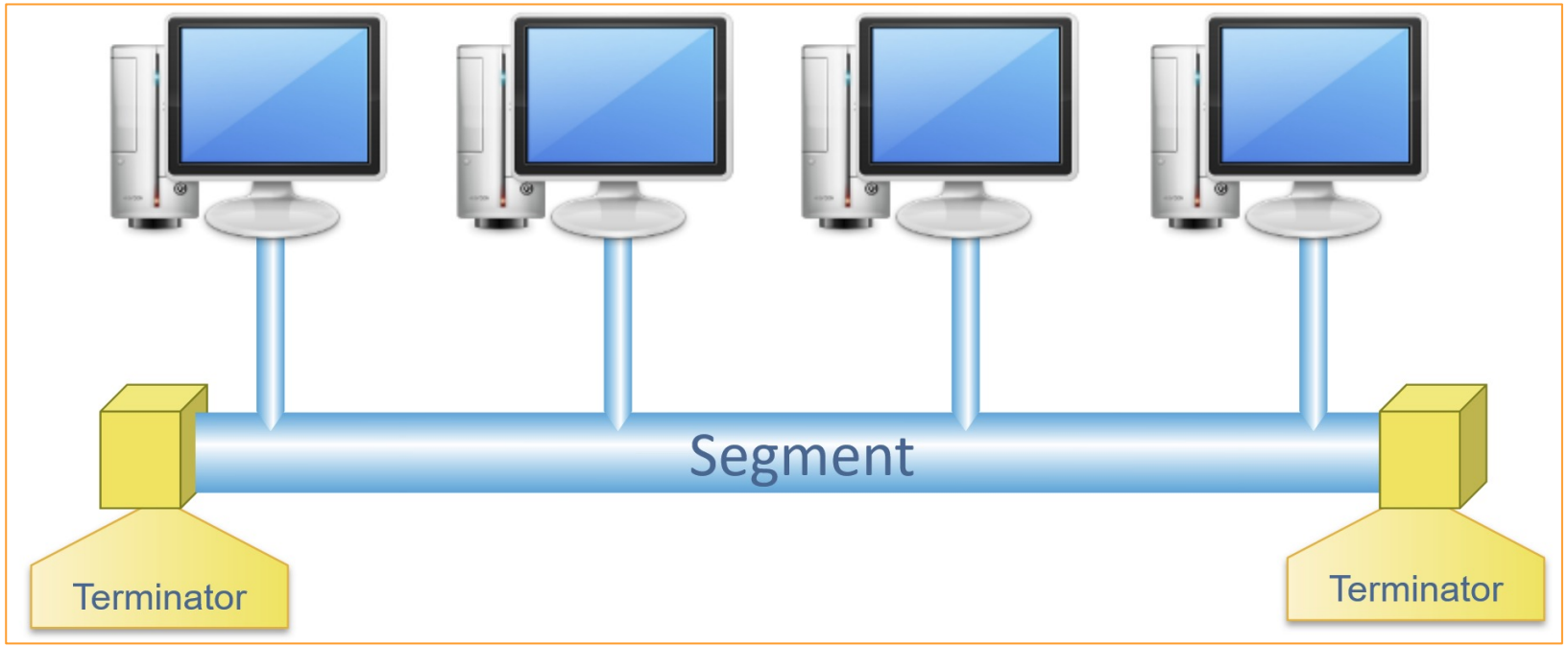


DOMAIN 4: COMMUNICATION AND NETWORK SECURITY

Transmission Media

Network Topologies - Bus

- Connected by a single line or backbone cable.



CISSP

DON

Tra

Ne

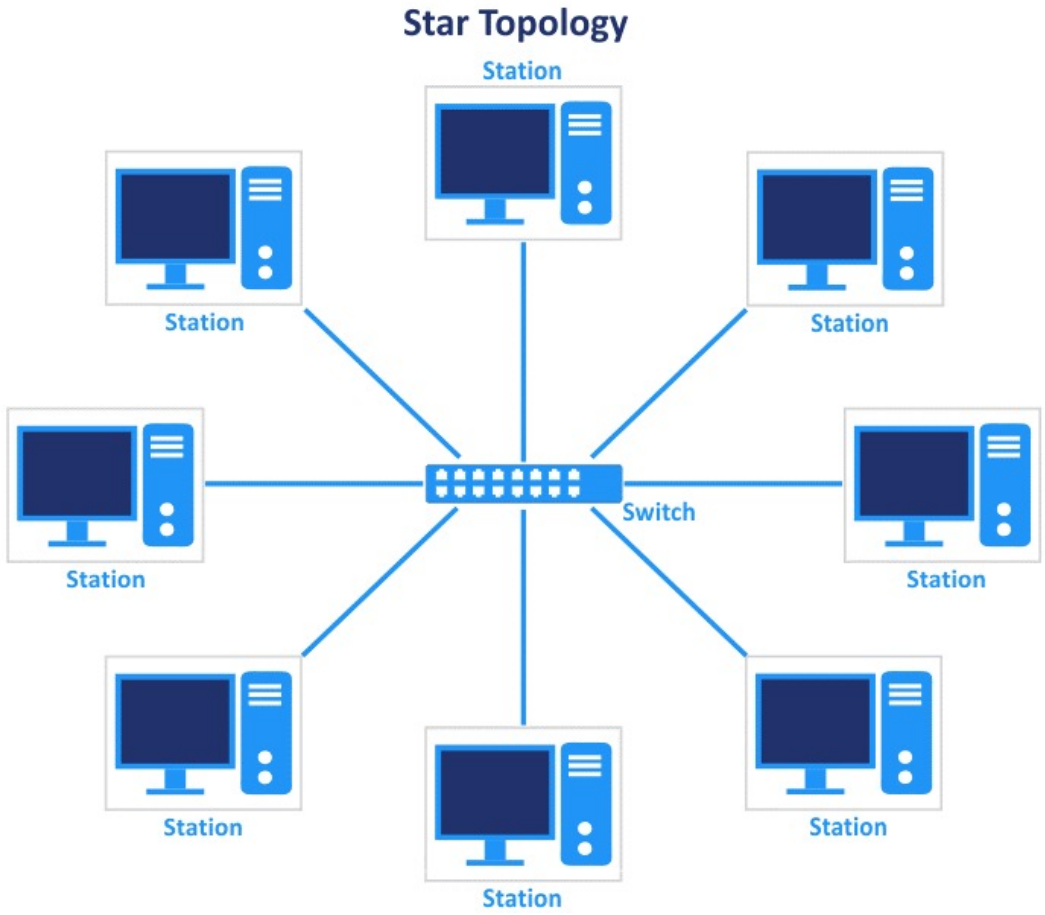
- C

DOMAIN 4: COMMUNICATION AND NETWORK SECURITY

Transmission Media

Network Topologies – Star

- All devices connect to a central system/controller.
- Usually a hub, switch, etc.
- Single point of failure is limited to a central system/controller.

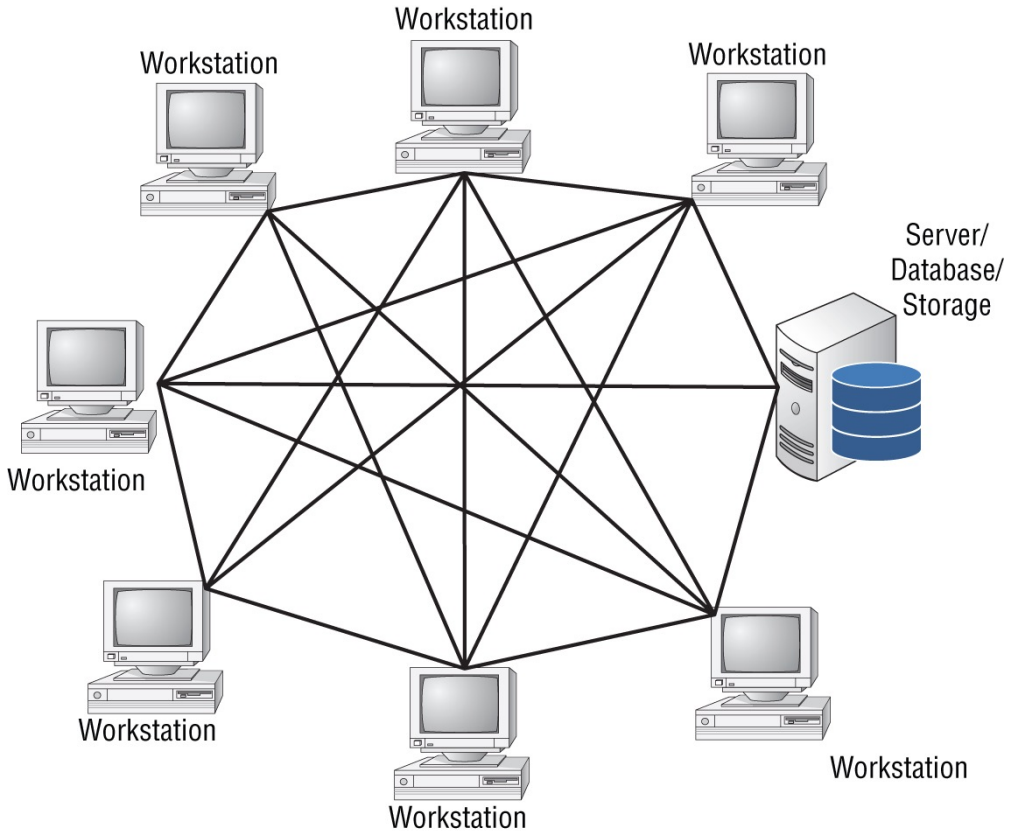


DOMAIN 4: COMMUNICATION AND NETWORK SECURITY

Transmission Media

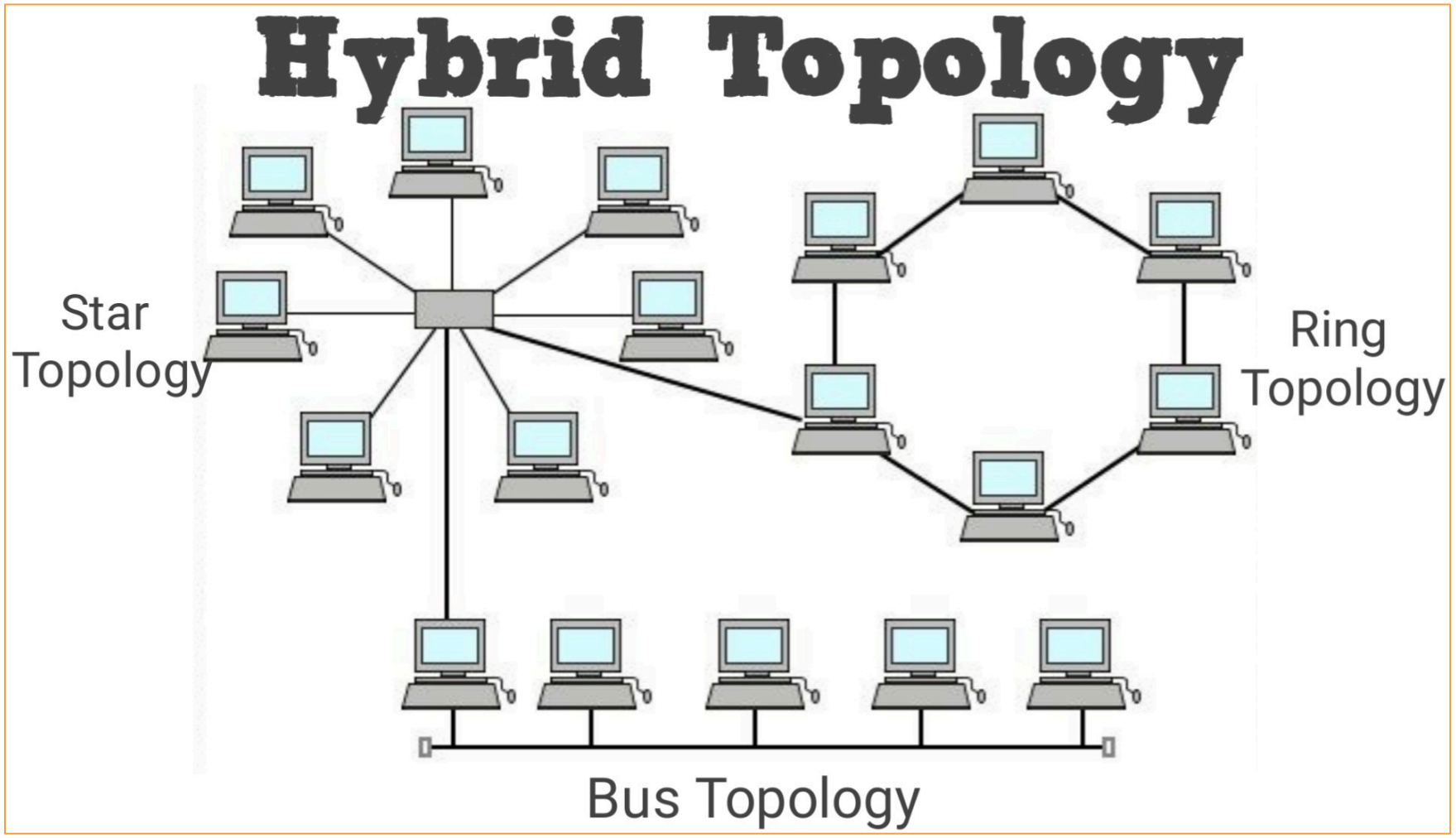
Network Topologies – Mesh

- **Full** – everything is connected to everything. Highly resilient, but very expensive.
- **Partial** – some things are connected to some things. Good for HA systems.



DOMAIN 4: COMMUNICATION AND NETWORK SECURITY

Transmission Media



DOMAIN 4: COMMUNICATION AND NETWORK SECURITY

Network Access Control

- Also referred to as NAC.
- Support network visibility and access management through **policy enforcement** on devices and users of corporate networks.
- **Deny network access** to noncompliant devices, place them in a **quarantined** area, or give them only **restricted access** to computing resources.

Two types of NAC, including the following:

- **Pre-admission** - evaluates access attempts and only allows entry to authorized devices and users.
- **Post-admission** - re-authenticates users trying to enter a different part of the network; also restricts lateral movement to limit the damage from cyber attacks.

CISSP® MENTOR PROGRAM – SESSION SEVEN

DOMAIN 4: COMMUNICATION AND NETWORK SECURITY

Network Access Control

Agent versus agentless

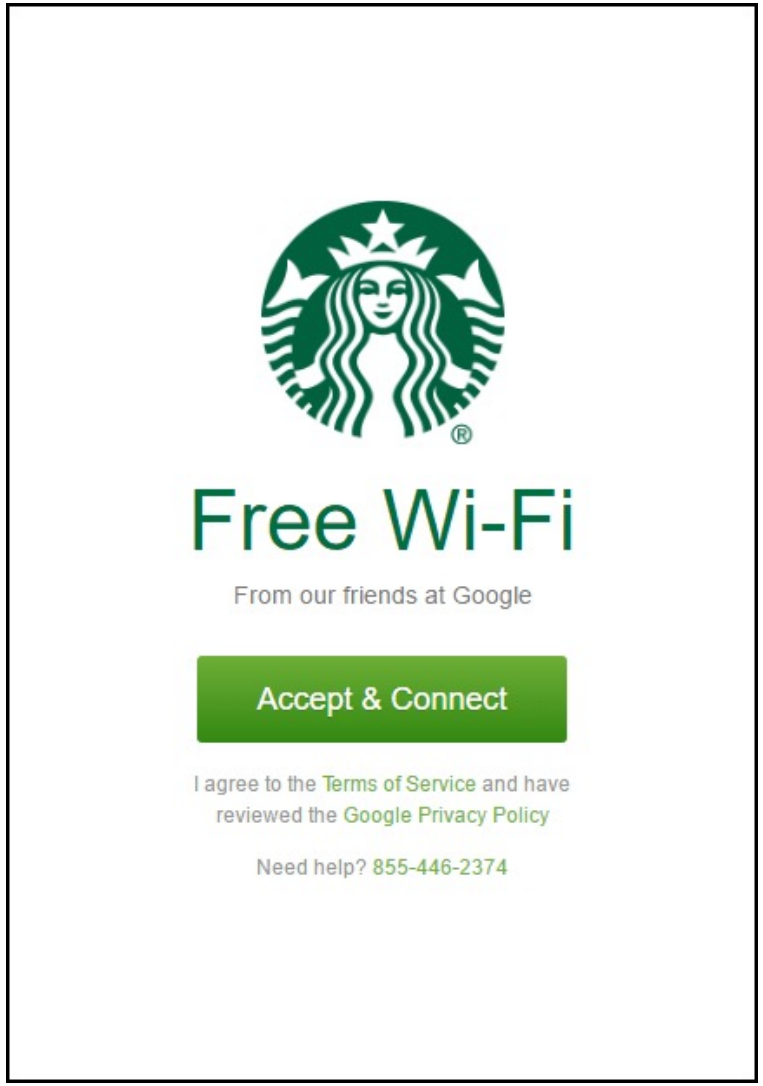
Out-of-band versus inline

Remediation

Quarantine

Captive portals

There are 1,000s of ways to implement NAC.



DOMAIN 4: COMMUNICATION AND NETWORK SECURITY

IMPLEMENT SECURE COMMUNICATION CHANNELS ACCORDING TO DESIGN

Voice - Private Branch Exchange (PBX)

- Enterprise-class phone system
- Internal switching network and a controller
- Uses embedded, proprietary software that contains customer-specified data and translations for routing voice, data, and video transmissions.

Securing the Other System: Basic PBX Functionality and Vulnerabilities
Brian L. Waldrop
GSEC Practical v1.2
April 24, 2001

https://www.giac.org/paper/gsec/671/securing-system-basic-pbx-functionality-vulnerabilities/101135#:~:text=However%2C%20a%20review%20of%20PBX,forwarding%2C%20and%20thru%2Ddialing.

Introduction

Hacking into a computer or data network is a well-known phenomenon and most organizations spend a great deal of time and money protecting the confidentiality,

DOMAIN 4: COMMUNICATION AND NETWORK SECURITY

IMPLEMENT SECURE COMMUNICATION CHANNELS ACCORDING TO DESIGN

Voice - Private Branch Exchange (PBX)

Common Threats To PBXs and Voice Mail Systems

- **Theft of Service** - The common motive for attackers, Toll Fraud.
- **Disclosure of information** - The disclosure of confidential and/or proprietary information, including conversations and system configuration data.
- **Data modification** - The illegal modification of system configuration data or records.
- **Unprivileged access** - Access by unauthorized users to gain control of system resources or privileges.
- **Denial of service** - Attacks that lead to the deterioration of service or suspension of functionality.
- **Traffic analysis** - A passive attack that allows phreakers to view calling patterns and make conclusions based on the source and destination of calls.

DOMAIN 4: COMMUNICATION AND NETWORK SECURITY

IMPLEMENT SECURE COMMUNICATION CHANNELS ACCORDING TO DESIGN

Voice - Private Branch Exchange (PBX)

Common Vulnerabilities

- **Physical Security** - Switchroom Security, System Printouts/Documentation, etc.
- **Remote Access** - most PBX and voice mail systems allow system administrators and/or switch vendors to remotely access system resources for administrative and maintenance functions.
- **Direct Inward System Access (DISA)** - most commonly abused system feature. DISA offers a convenient means for offsite employees to place calls to internal extensions, private network locations, and external numbers by accessing the PBX
- **Call Forwarding**
- **Thru-dialing**

CISSP® MENTOR PROGRAM – SESSION SEVEN

DOMAIN 4: COMMUNICATION AND NETWORK SECURITY

IMPLEMENT SECURE COMMUNICATION CHANNELS ACCORDING TO DESIGN

Voic

Comm

- **Phy** cumentation, etc.
- **Rem** m adm m resources for a
- **Dire** d system feat o place calls to in umbers by acce
- **Call**
- **Thru**

DOMAIN 4: COMMUNICATION AND NETWORK SECURITY

IMPLEMENT SECURE COMMUNICATION CHANNELS ACCORDING TO DESIGN

Voice – Plain Old Telephone Service (POTS)

- Residential networks and some businesses
- Carry human voice over a bidirectional analog telephone interface
- Voice communications are vulnerable to interception, eavesdropping, tapping, and other exploitations

POTS and PBX security controls rely heavily on physical controls

DOMAIN 4: COMMUNICATION AND NETWORK SECURITY

IMPLEMENT SECURE COMMUNICATION CHANNELS ACCORDING TO DESIGN

Voice – Voice over Internet Protocol (VoIP)

- Encapsulate voice communications and multimedia sessions over IP networks
- When configured correctly VoIP is generally more secure than landlines.

CISSP® MENTOR PROGRAM – SESSION SEVEN

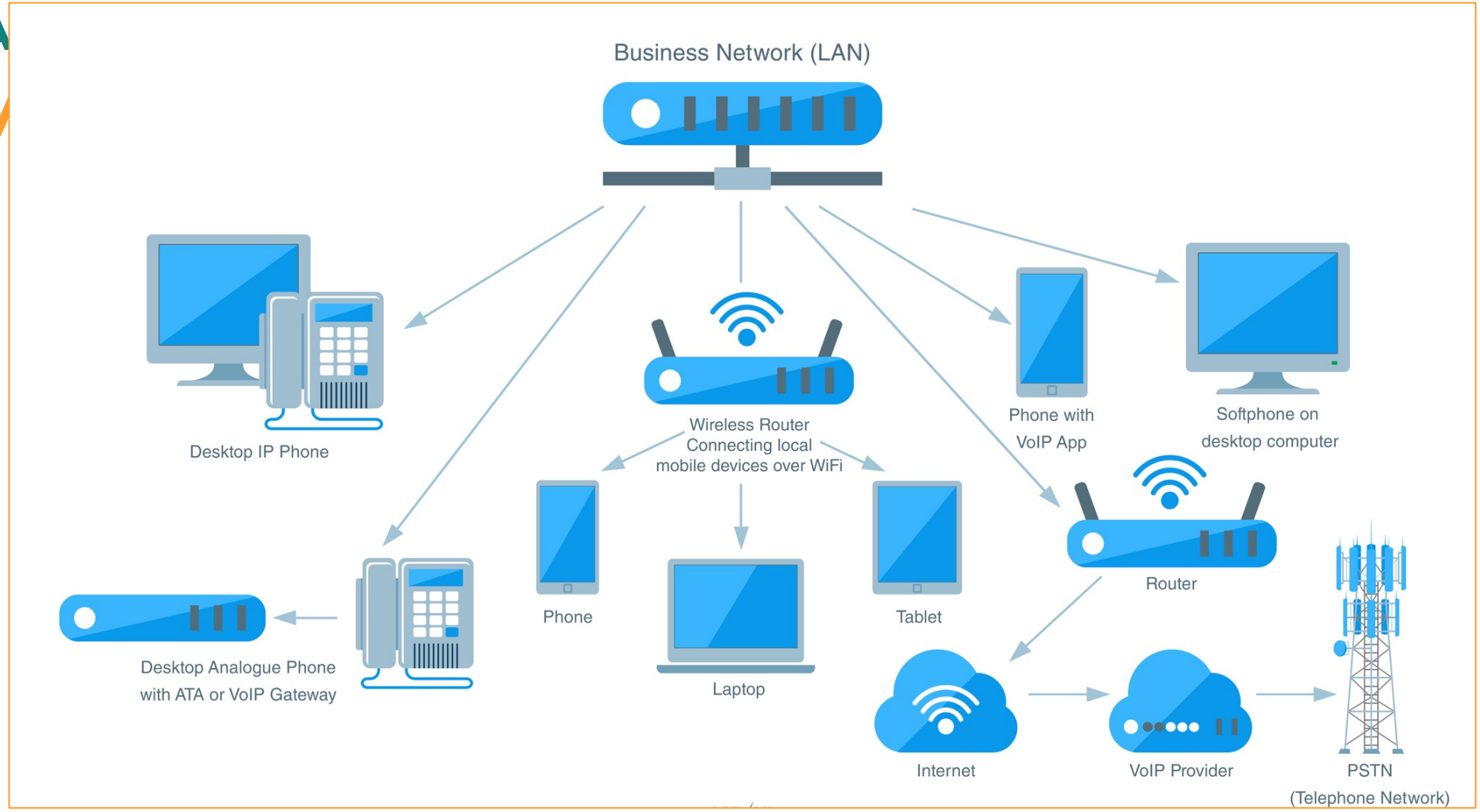
DOMAIN 4: COMMUNICATION AND NETWORK SECURITY

IMPLEMENT SECURE COMMUNICATION CHANNELS

A

V

-
-



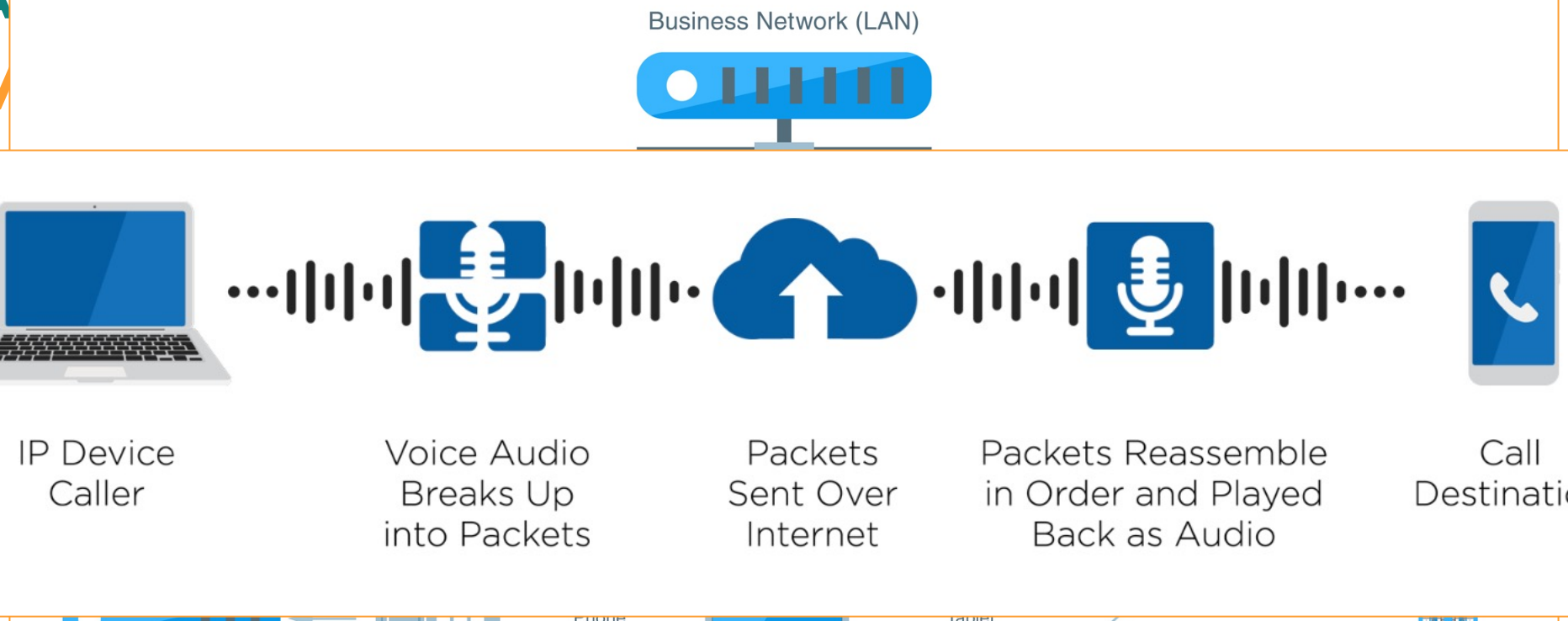
CISSP® MENTOR PROGRAM – SESSION SEVEN

DOMAIN 4: COMMUNICATION AND NETWORK SECURITY

IMPLEMENT SECURE COMMUNICATION CHANNELS

A

V



DOMAIN 4: COMMUNICATION AND NETWORK SECURITY

IMPLEMENT SECURE COMMUNICATION CHANNELS ACCORDING TO DESIGN

Voice – Voice over Internet Protocol (VoIP)

- When voice data packets are transferred from the sender to the recipient, they use an IP transport protocol called the **SRTP** (Secure Real-Time Transport Protocol.)
- SRTP is a cryptographic protocol that applies the Advanced Encryption Standard (AES) to data packets, provides message authentication, and offers additional protection against potential replay attacks.
- In addition to SRTP, VoIP providers use another form of encryption called Transport Layer Security (TLS) or SIP over TLS to protect additional call information.

DOMAIN 4: COMMUNICATION AND NETWORK SECURITY

IMPLEMENT SECURE COMMUNICATION CHANNELS ACCORDING TO DESIGN

Voice – Voice over Internet Protocol (VoIP)

- Packet Sniffing and Black Hole Attacks
- DDoS Attacks
- Vishing
- Malware and Viruses
- Phreaking Attack - a type of fraud where the VoIP system is used to make long-distance calls, change calling plans, add more account credits, and make any additional phone calls they want — all on the victim's dime.
- SPIT, or Spam over IP Telephony
- Voice over Misconfigured Internet Telephones, or VOMIT, (gross, we know) is a VoIP hacking tool.

DOMAIN 4: COMMUNICATION AND NETWORK SECURITY

Multimedia Collaboration

Remote Meeting

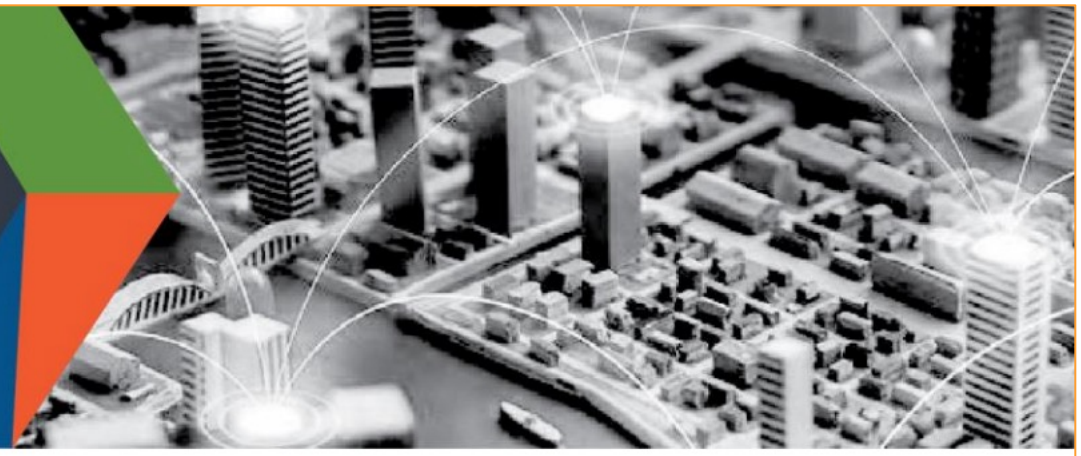
Common examples of threats or risks include the following:

- Threats to privacy, identification, or Personally Identifiable Information (PII)
- Risks to data from data theft or breaches
- Risks to confidential business or corporate information or intellectual property
- Meeting hijackings
- Access to confidential meeting recordings

https://www.cisa.gov/sites/default/files/publications/CISA_Guidance_for_Securing_Video_Conferencing_S508C.pdf

CISA
CYBER+INFRASTRUCTURE

DEFEND TODAY, SECURE TOMORROW



GUIDANCE FOR SECURING VIDEO CONFERENCING

This product is for organizations and individual users leveraging videoconferencing tools, some of whom are remotely working for the first time.

As the authority for securing telework, the **Cybersecurity and Infrastructure Security Agency (CISA)** established this product line with cybersecurity principles and practices that individuals and organizations can follow to video conference more securely. Although CISA is providing this general risk advisory guidance, individuals and organizations are responsible for their own risk assessments of specific systems and software. For optimum risk mitigation, organizations should implement measures at both the organizational and user levels.

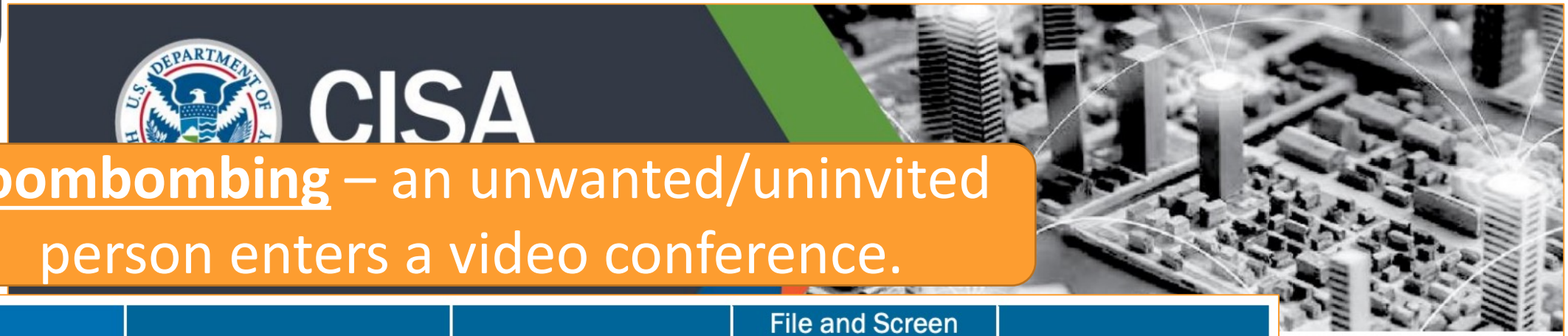
BACKGROUND

- The Federal Government, state and local governments, the private sector, and general public have pivoted to widescale remote work and online collaboration

FOUR PRINCIPLES AND TIPS TO SECURE VIDEO CONFERENCING

1. CONNECT SECURELY

Risk: The initial settings for home Wi-Fi networks and many video



Zoombombing – an unwanted/uninvited person enters a video conference.

Product	Control Access	Connect Securely	File and Screen Sharing and Recording	Update Versions
Zoom	Managing group policy in Zoom			
	✓ Assigning roles ✓ Enable waiting rooms ✓ Enable passwords ✓ Identify guest participants ✓ Enable two-factor authentication	✓ Encryption ✓ Security settings ✓ Audio watermark	✓ Limiting file types ✓ Managing meeting participants (including screen sharing)	✓ Updates for Windows ✓ Updates for MacOS ✓ Updates for Android ✓ Updates for iOS

emotely working for

this product line
ore securely.
r their own risk
easures at both

URE VIDEO

BACKGROUND

- The Federal Government, state and local governments, the private sector, and general public have pivoted to widescale remote work and online collaboration

CONFERENCING

1. CONNECT SECURELY

Risk: The initial settings for home Wi-Fi networks and many video

DOMAIN 4: COMMUNICATION AND NETWORK SECURITY

Multimedia Collaboration

Instant Messaging

Top Risks (https://www.networkworld.com/article/2323048/top-5-im-security-risks.html)

1. Viruses and worms over IM.

Out of the top 50 viruses and worms over the past six months, 19 of them used peer-to-peer or IM applications. Most viruses are sent through file transfers, which bypass traditional gateway and anti-virus security. Public IM clients also have publicized vulnerabilities, where flaws such as buffer overflows and boundary condition errors have been exploited to spread viruses, worms or denial-of-service attacks.

DOMAIN 4: COMMUNICATION AND NETWORK SECURITY

Multimedia Collaboration

Instant Messaging

Top Risks (https://www.networkworld.com/article/2323048/top-5-im-security-risks.html)

2. Identity theft/authentication spoofing.

Public IM systems let individuals create anonymous identities, which do not map to e-mail addresses. IDs can be created even if the IDs and domains are not owned by that individual ("billgates" or "johnchambers," for example). Spoofing creates risk, as these IDs can be used maliciously, outside the control of the IT security department.

DOMAIN 4: COMMUNICATION AND NETWORK SECURITY

Multimedia Collaboration

Instant Messaging

Top Risks (https://www.networkworld.com/article/2323048/top-5-im-security-risks.html)

3. Firewall tunneling.

IM clients find ways to tunnel through firewalls, creating risk. Most IM services come through well-publicized ports (5190 for AOL Instant Messenger, 1863 for MSN and 5050 for Yahoo), but IM clients also can exploit any open port on the firewall, including those used by other applications (such as Port 80 for Web and HTTP traffic). Some clients also can connect via peer-to-peer connections or establish connections on randomly negotiated ports.

DOMAIN 4: COMMUNICATION AND NETWORK SECURITY

Multimedia Collaboration

Instant Messaging

Top Risks (https://www.networkworld.com/article/2323048/top-5-im-security-risks.html)

4. Data security leaks.

Unmonitored content leaving the corporation without the knowledge of the information security department introduces legal and competitive risk (such as a CFO sending a confidential spreadsheet via IM without an audit trail). File transfer over IM is a powerful way to send information beyond the tracing capabilities of the IT department. The lack of content filtering and archiving makes it difficult for IT to discover potential breaches of policy or to hold individuals accountable.

DOMAIN 4: COMMUNICATION AND NETWORK SECURITY

Multimedia Collaboration

Instant Messaging

Top Risks (https://www.networkworld.com/article/2323048/top-5-im-security-risks.html)

5. Spim.

IMlogic says that 5% to 7% of IM traffic today is spim (instant messaging spam). Spim can be more disruptive than e-mail spam, as it is more intrusive (the pop-up spim interrupts the user) and generally of a more sexually offensive nature (leading to human resources and legal risk).

DOMAIN 4: COMMUNICATION AND NETWORK SECURITY

Multimedia Collaboration

Email

- Arguably the #1 entry point into corporate networks (as the beginning of the attack “vector”).
- Social engineer’s paradise and an easy way to get files into an organization.
  - **SMTP** (TCP 25, sometime TCP 587), a store and forward protocol for sending email.
  - **POP3** (TCP 110, TCP 995 for SSL/TLS) - mail protocol used to retrieve mail from a remote server to a local email client. POP3 copies the mail from the remote server into the local mail client.
  - **IMAP** (TCP 143, TCP 993 for SSL/TLS) - mail protocol used to access a mailbox on a remote server from a local email client. IMAP can be more complex but provide more convenience for syncing across multiple devices.

DOMAIN 4: COMMUNICATION AND NETWORK SECURITY

Multimedia Collaboration

Email

- Sendmail, Exchange, Office 365, Gmail, etc.
- Attacks are sometimes focused on the server/service itself, and the client(s).
- Vulnerabilities typically come from:
  - Poor configuration.
  - Unpatched (or outdated) systems.
  - User (admin and/or end) mistakes.
- Ensure server is not an open relay, require authentication and DNS protections.

DOMAIN 4: COMMUNICATION AND NETWORK SECURITY

Multimedia Collaboration

Email – start with policy…

- **Acceptable use**: These are general guidelines for what email can be used for, which may (or may not) include minimal personal use.
- **Access control**: Access should be restricted to individual inboxes and archives.
- **Privacy**: Users of a corporate email system should generally be accustomed to having no expectation of privacy.
- **Email backup and retention policies**: Backups and archives are needed for data recovery, legal proceedings, and many audits.

DOMAIN 4: COMMUNICATION AND NETWORK SECURITY

Multimedia Collaboration

Email – start with policy…

- **Acceptable use**: These are general ~~guidelines~~ **requirements** for what email can be used for, which may (or may not) include minimal personal use.
- **Access control**: Access should be restricted to individual inboxes and archives.
- **Privacy**: Users of a corporate email system should generally be accustomed to having no expectation of privacy.
- **Email backup and retention policies**: Backups and archives are needed for data recovery, legal proceedings, and many audits.

DOMAIN 4: COMMUNICATION AND NETWORK SECURITY

Multimedia Collaboration

Email – (some) other considerations

Secure Multipurpose Internet Mail Extensions (S/MIME)

- Widely accepted protocol for sending digitally signed and encrypted messages.
- Uses public key encryption and digital signatures to enable authentication and confidentiality for emails
- X.509 digital certificates are used to provide authentication
- Public Key Cryptography Standard (PKCS) encryption is used to provide privacy.

Two types of messages can be formed using S/MIME:

- **Signed messages**: To provide integrity, sender authentication, and nonrepudiation of the sender
- **Enveloped messages**: To provide integrity, sender authentication, and confidentiality

DOMAIN 4: COMMUNICATION AND NETWORK SECURITY

Multimedia Collaboration

Email – (some) other considerations

MIME Object Security Services (MOSS)

- Authentication, confidentiality, integrity and nonrepudiation services for email messages
- Uses Message Digest 2 (MD2) and MD5 algorithms; Rivest, Shamir, and Adelman (RSA) public key; and Data Encryption Standard (DES) to provide authentication and encryption services.

Privacy Enhanced Mail (PEM)

- Provides authentication, integrity, confidentiality, and nonrepudiation.
- Also uses RSA, DES, and X.509.

DOMAIN 4: COMMUNICATION AND NETWORK SECURITY

Multimedia Collaboration

Email – (some) other considerations

DomainKeys Identified Mail (DKIM)

- Validates mail was sent by an organization through verification of domain name identity.
- Relies on public keys and digital signing

Pretty Good Privacy (PGP)

- Public-private key system that uses a variety of encryption algorithms to encrypt email messages
- Used for signing, encrypting, and decrypting texts, e-mails, files, directories, and whole disk partitions and to increase the security of e-mail communications.
- Developed by Phil Zimmerman in 1991
- Not a standard.

DOMAIN 4: COMMUNICATION AND NETWORK SECURITY

Multimedia Collaboration

Remote Access

Many types of "remote access"

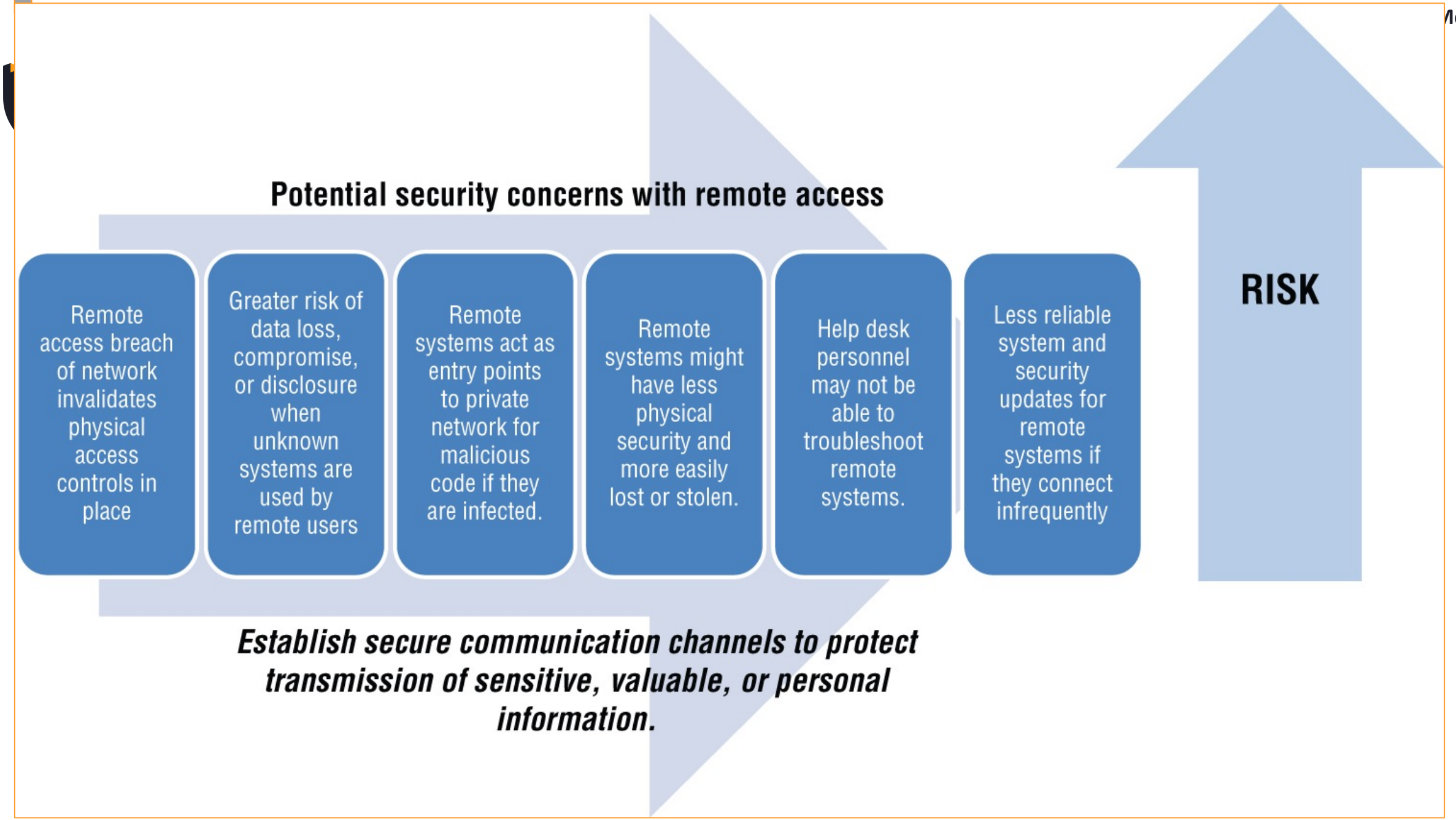
- **Service specific** - Outlook Web Access (OWA), various terminal services, time and attendance applications, etc.
- **Remote control** – Remote Desktop Protocol (RDP, TCP 3389), Windows Terminal Server, and numerous other applications.
- **Screen scraping** – the ability to copy data off the screen, from one application into another. Great risk of unauthorized disclosure of sensitive information.

DOMAIN 4: COMMUNICATION AND NETWORK SECURITY

Multimedia Collaboration

Remote Access Security Management

- A **strong authentication** system is required; multifactor authentication is the standard to protect sensitive information.
- Limit remote access to **only those who need it** and who routinely use it.
- Implement **encryption for data in transit**, to include one or more of these examples: VPNs, SSL, TLS, SSH, and IPSec.
- Understand that a **VPN is not a complete security solution**; end users who can authenticate and establish a VPN may be accessing the network with an infected computer or mobile device.



DOMAIN 4: COMMUNICATION AND NETWORK SECURITY

Multimedia Collaboration

Remote Access Authentication

Centralized Remote Authentication Services - **Remote Authentication Dial-In User Service or "RADIUS"**

- A **RADIUS Client** (or Network Access Server) is a networking device (like a VPN concentrator, router, switch) that is used to authenticate users.
- A **RADIUS Server** is a background process that runs on a UNIX or Windows server. It lets you maintain user profiles in a central database. Hence, if you have a RADIUS Server, you have control over who can connect with your network.
- All servers have AAA capabilities (Authentication, Authorization, and Accounting)

DOMAIN 4: COMMUNICATION AND NETWORK SECURITY

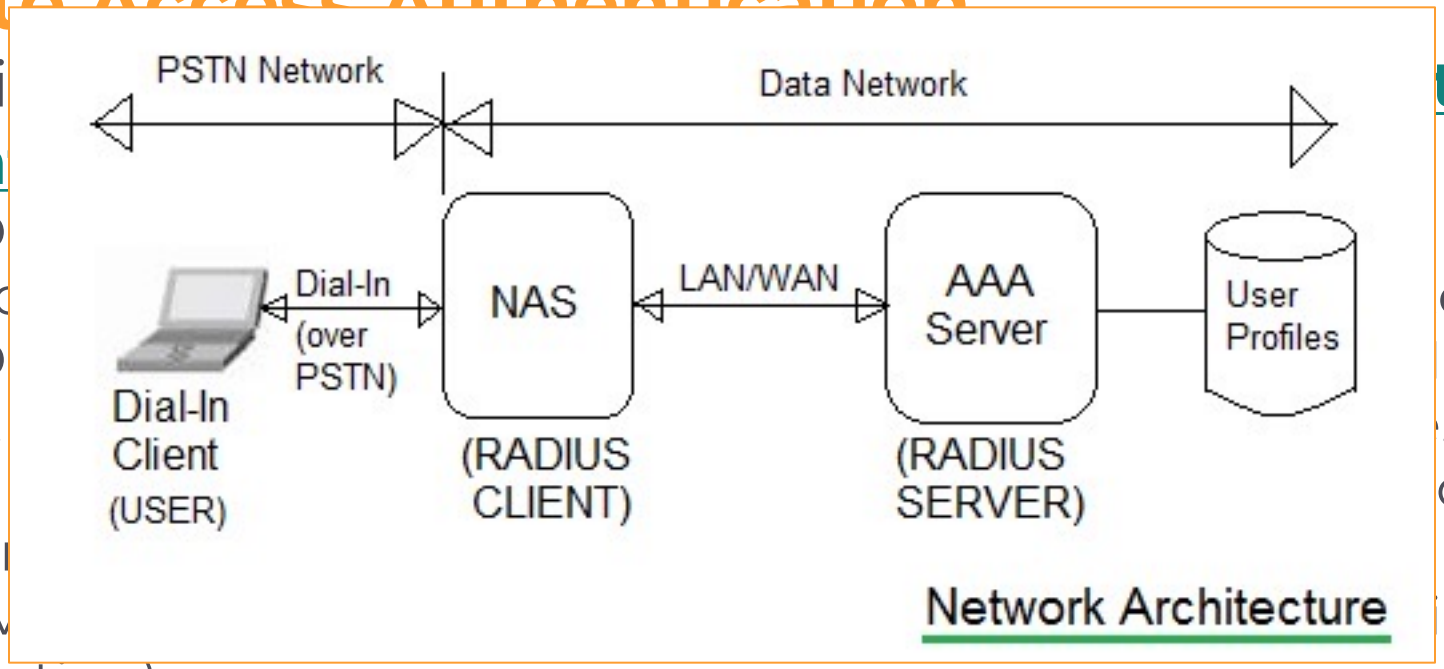
Multimedia Collaboration

Remote Access Authentication

Centrali… …te

Authen…

- A **RAD**… …device (like a VPN c… …e users.
- A **RAD**… …IX or Windows server. …. Hence, if you have a… …ct with your netwo…
- All serv… …on, and Accounting)



Network Architecture

DOMAIN 4: COMMUNICATION AND NETWORK SECURITY

Multimedia Collaboration

Remote Access Authentication

Centralized Remote Authentication Services - **Diameter**

Evolved from RADIUS

Radius protocol	Diameter protocol
The full form is Remote Authentication Dual In User Service	It is enhanced radius protocol. It is successor to radius protocol.
It uses UDP.	It uses TCP/SCTP (i.e. Stream Control Transmission Protocol).
It is unreliable protocol as it lacks in reliability, ordering and data integrity.	It is reliable protocol as all the AAA nodes exchange messages and use positive and negative feedback mechanism for each messages.
It is defined in RFC 2865.	It is defined in RFC 6733 and RFC 3588.
Applications are Network Access, IP Mobility etc.	Applications are NAS, mobile IP, credit controls, 3G, SIP, EAP etc.

DOMAIN 4: COMMUNICATION AND NETWORK SECURITY

Multimedia Collaboration

Remote Access Authentication

Centralized Remote Authentication Services - **TACACS**

- Three versions: TACACS, Extended TACACS (XTACACS), and TACACS+
- TACACS integrates the authentication and authorization processes. XTACACS keeps the authentication, authorization, and accounting processes separate. TACACS+ improves XTACACS by adding two-factor authentication. TACACS+ is the most current and relevant version of this product line.
- Developed by Cisco, but an open standard.

CISSP®

DOM ITY

Mul

Rem

Cent

- Th), and
- TA ion
- pr CACS+
- au ion.
- im his
- TA
- pr
- De

Figure 1: RADIUS vs. TACACS+

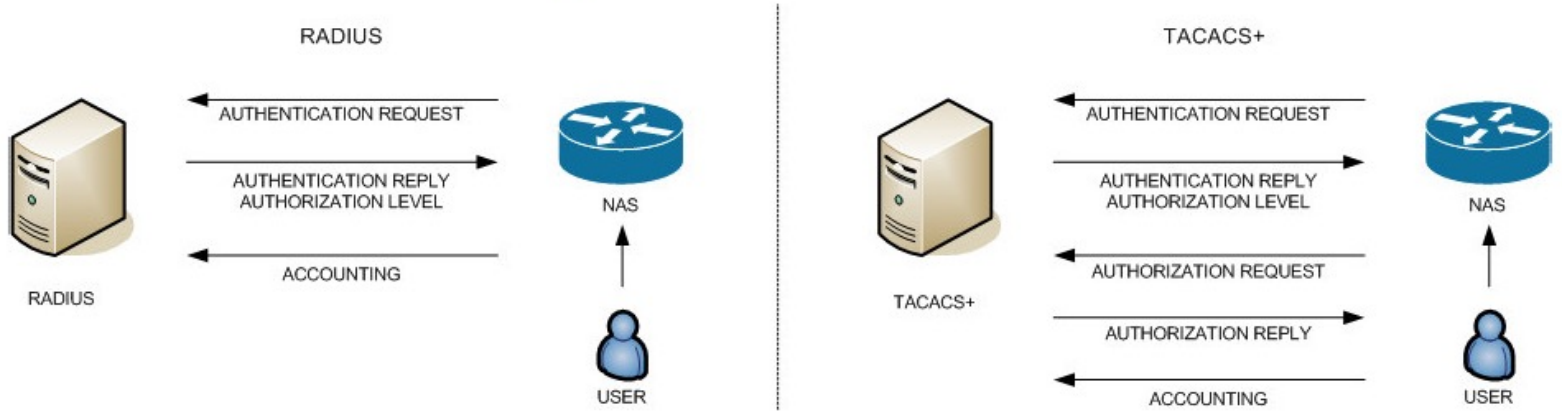


Table 1: RADIUS vs. TACACS+

RADIUS	TACACS+
Combines authentication & authorization.	Separates all 3 elements of AAA, making it more flexible.
Encrypts only the password.	Encrypts the username and password.
Requires each network device to contain authorization configuration.	Central management for authorization configuration.
No command logging.	Full command logging.
Minimal vendor support for authorization.	Supported by most major vendors.
UDP- Connectionless UDP ports 1645/1646, 1812/1813	TCP- Connection oriented TCP port 49
Designed for subscriber AAA	Designed for administrator AAA

DOMAIN 4: COMMUNICATION AND NETWORK SECURITY

Multimedia Collaboration

Virtual Private Network - Point-to-Point Tunneling Protocol (PPTP)

- Data link layer (layer 2) used on IP networks.
- One of the oldest protocols still being used by VPNs today, developed by Microsoft and released with Windows 95.
- Easy to configure, requiring only a username, password, and server address to connect to the server.
- Fast because of its low encryption level, but one of the least secure protocols.
- Known vulnerabilities dating as far back as 1998, and the absence of strong encryption – government agencies like the NSA have been able to compromise.

DOMAIN 4: COMMUNICATION AND NETWORK SECURITY

Multimedia Collaboration

Virtual Private Network - Point-to-Point Tunneling Protocol (PPTP)

- Developed from the dial-up protocol called Point-to-Point Protocol (PPP)
- Same authentication protocols supported by PPP:
  - Microsoft Challenge Handshake Authentication Protocol (MS-CHAP)
  - CHAP
  - PAP
  - EAP
  - Shiva Password Authentication Protocol (SPAP)
- Session establishment for PTPP is not encrypted.

DOMAIN 4: COMMUNICATION AND NETWORK SECURITY

Multimedia Collaboration

Virtual Private Network - Secure Socket Tunneling Protocol (SSTP)

- Transport internet data through the Secure Sockets Layer or SSL, is supported natively on Windows

DOMAIN 4: COMMUNICATION AND NETWORK SECURITY

Data Communications

Frame Relay

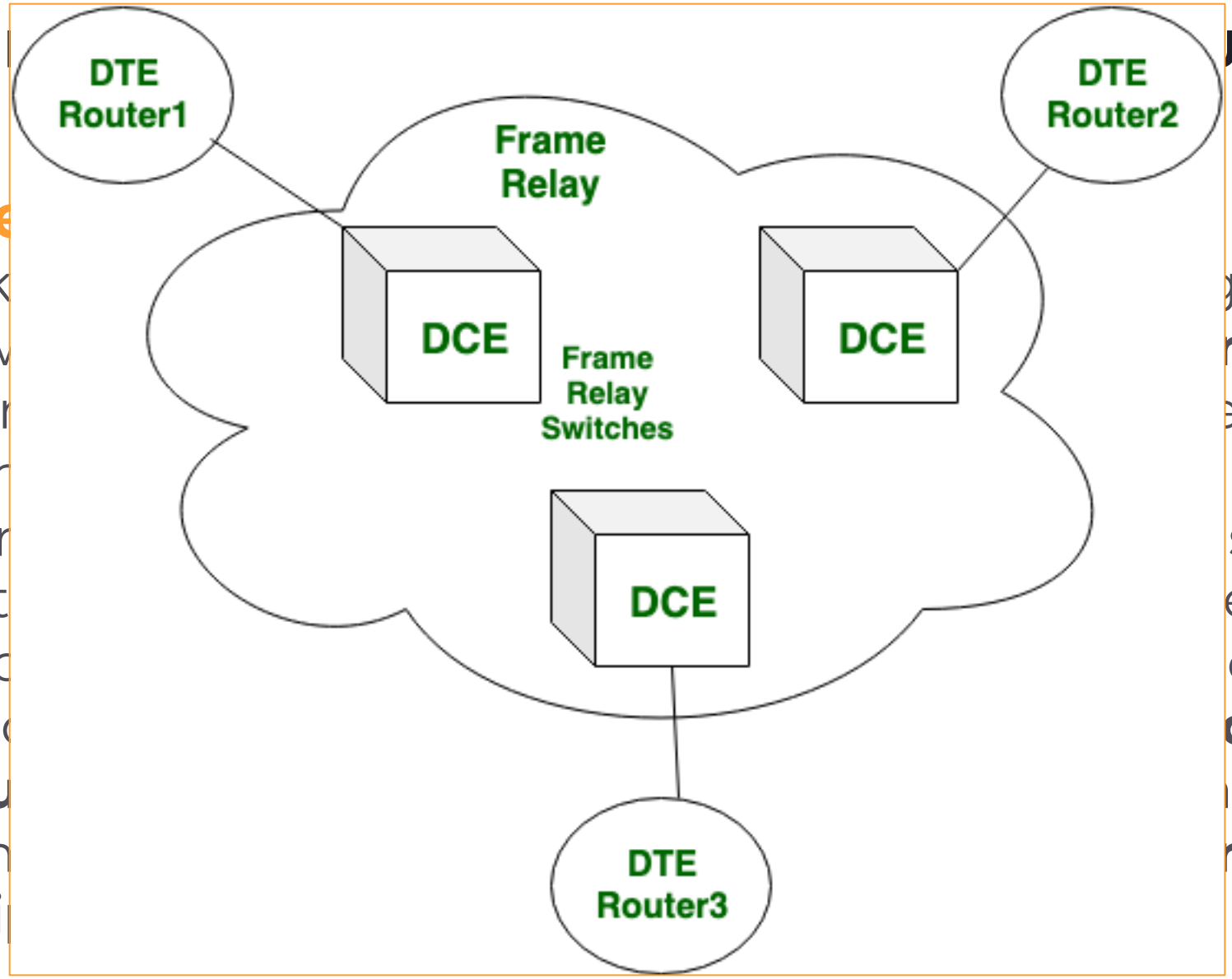
- Packet switched wide area networking, connecting networks operating at **physical and data link layers**.
- Often serves to connect LANs with major backbones.
- Connects separate WANs and private network environments with leased lines over T-1 connections.
- Started as an extension of ISDN, integrating a packet-switched networking over circuit-switched technology.
- Devices performing frame relay services are called **data circuit-terminating equipment (DCE)**. Devices that connect to the frame relay DCEs are called **data terminal equipment (DTE)**.

DOMAI URITY

Data

Frame

- Pack g
  netw rs.
- Ofter es.
- Conr
  envir s.
- Start et-
  swit ogy.
- Devi data
  circu t
  conn rminal
  equi



DOMAIN 4: COMMUNICATION AND NETWORK SECURITY

Data Communications

Asynchronous Transfer Mode (ATM)

- High-speed standard supporting voice and data.
- Designed to integrate telecommunication and computer networks.
- Normally used by ISPs on their private long- distance networks.
- Operates mostly at the data link layer (layer 2) and runs over fiber or twisted-pair cable.
- No routing, uses special-purpose hardware called ATM switches to establish point-to-point connections.
- ATM “cells” are 53-bytes.

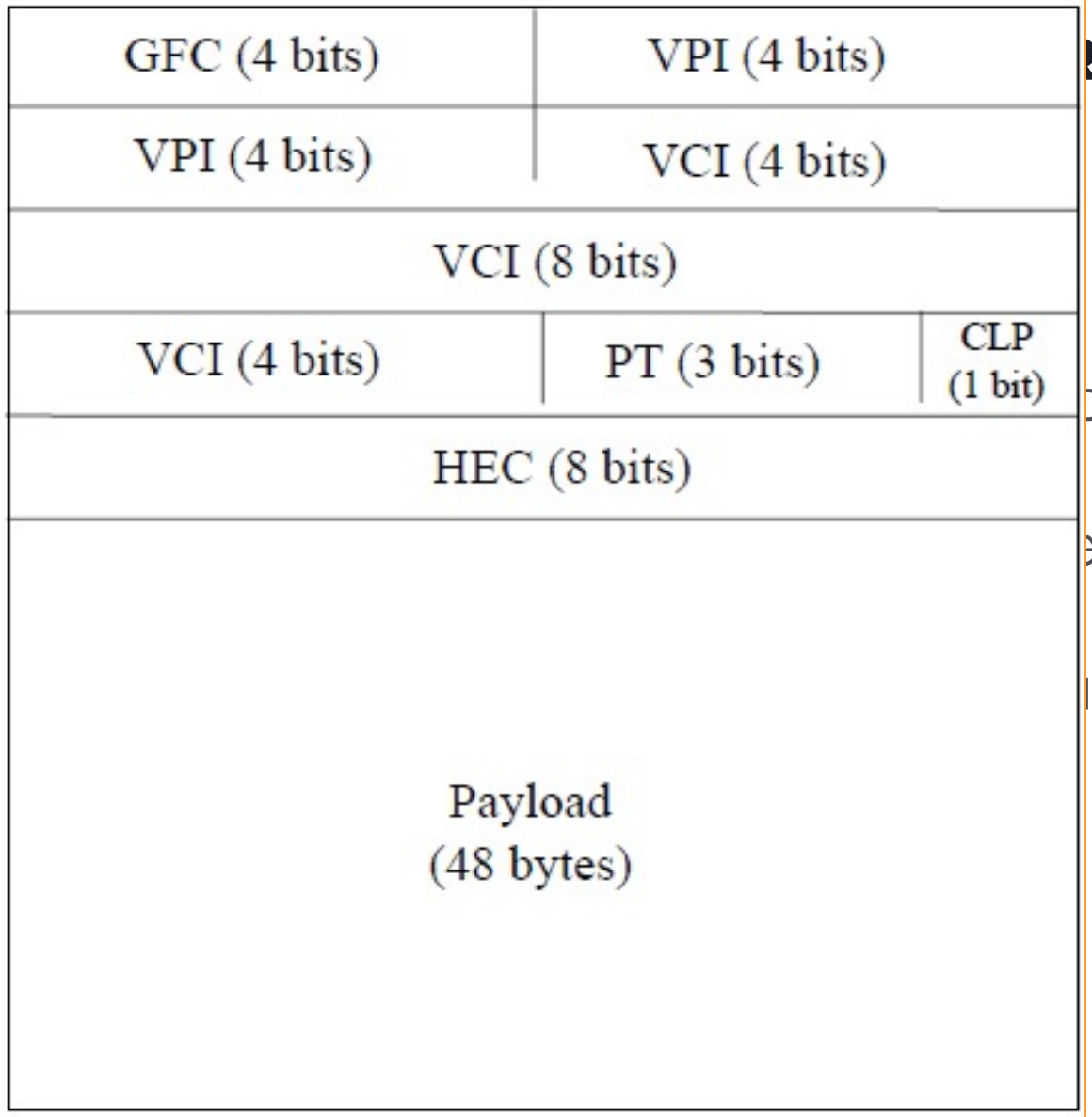
DOMA RITY

Data

Asyn

- Hig
- Des net
- Nor net
- Op fibe
- No swi
- ATM

ATM cell header



DOMAIN 4: COMMUNICATION AND NETWORK SECURITY

Data Communications

Asynchronous Transfer Mode (ATM)

- Performance often expressed in the form of optical carrier (OC) levels, written as “OC-xxx.”
  - OC-192, 10 Gbps
  - OC-3 (more common), 155 Mbps
  - OC-12, 622 Mbps
- Quality of Service (QoS). There are four basic types:
  - **Constant bit rate (CBR)**: A peak cell rate (PCR) is specified, which is constant.
  - **Variable bit rate (VBR)**: An average or sustainable cell rate (SCR) is specified, which can peak at a certain level, a PCR, for a maximum interval before being problematic.
  - **Available bit rate (ABR)**: A minimum guaranteed rate is specified.
  - **Unspecified bit rate (UBR)**: Allocation to remaining transmission capacity.

CISSP® MENTO

DOMAIN 4 CURITY

Data C

Asynch

- Perform cal carrier (OC) lev
  - OC-
  - OC-
  - OC-
- Quality es:
  - **Cons** hich is const
  - **Varia** CR) is speci mum interval befor
  - **Avail** cified.
  - **Unsp** sion capacity.

CISSP® MENTOR PROGRAM – SESSION SEVEN

SESSION 7 – POR FIN!

Homework:

- Review Domain 4 and start moving on to Domain 5.
- Take practice tests.
- Review at least two of the references we provided in this class (download for later use).
- Post at least one question/answer in the Slack Channel.

See you Wednesday!

2022

Class #7 – Domain 4

Evan Francen

Evan Francen – FRSecure and SecurityStudio Co-Founder & CEO