

Common Protocols and Services

Christopher Rees

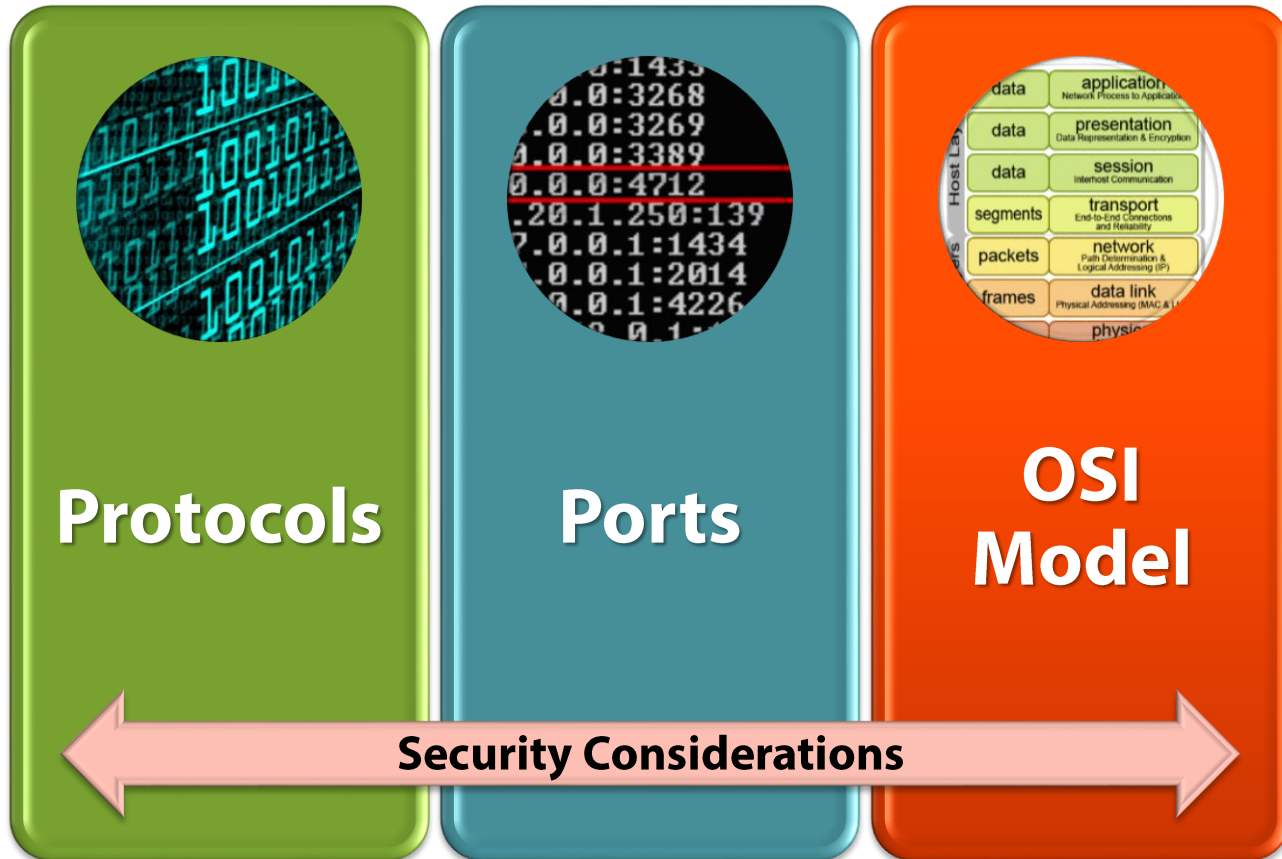
<https://www.linkedin.com/in/cdrees>

@cdrees



pluralsight 
hardcore dev and IT training

Common Protocols and Services



Module Overview

Protocols

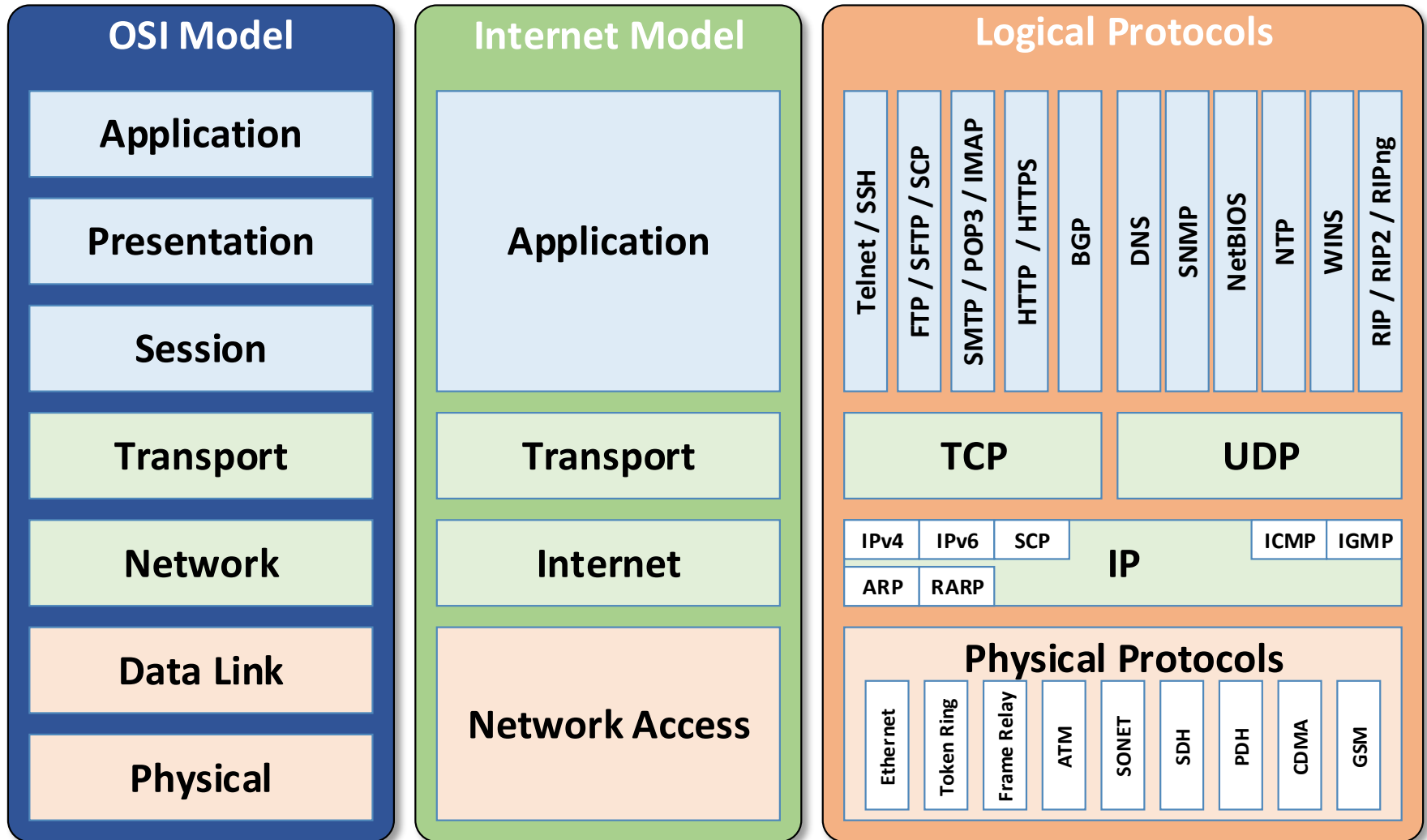
- IPsec
- SNMP
- SSH
- DNS
- TLS
- SSL
- TCP/IP
- FTPS
- HTTPS
- SCP
- ICMP
- IPv4
- IPv6
- iSCSI
- Fibre Channel
- FCoE
- FTP
- SFTP
- TFTP
- TELNET
- HTTP
- NetBIOS

Ports

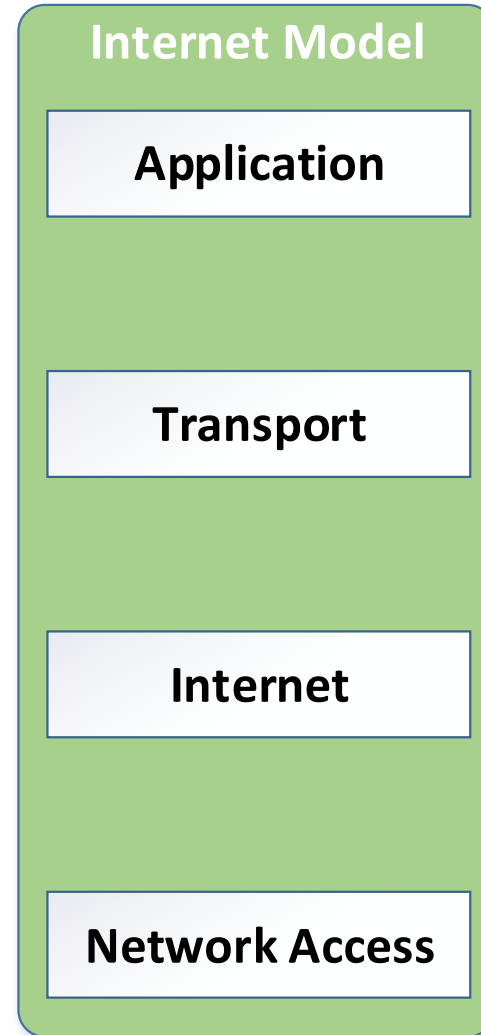
- 21
- 22
- 25
- 53
- 80
- 110
- 139
- 143
- 443
- 3389

- **OSI Relevance** (where it all fits)
- **Security Considerations**

OSI Model vs. Internet Model



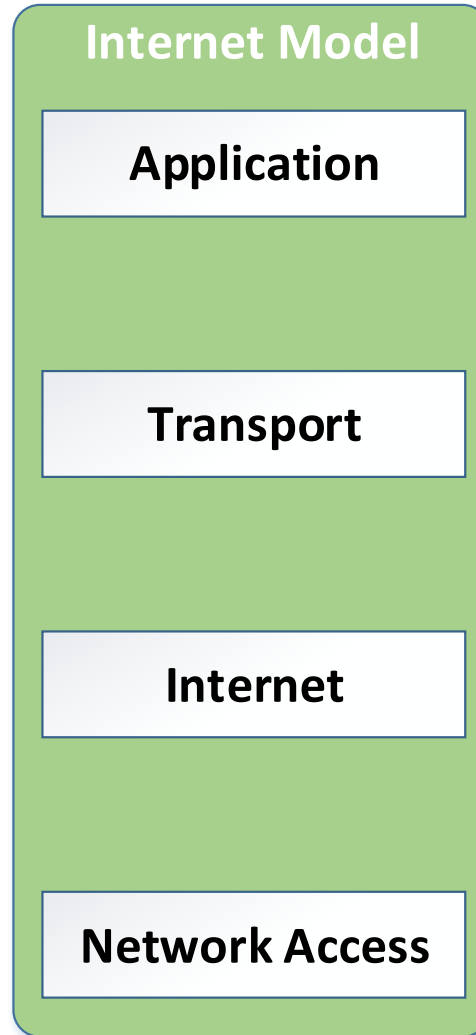
Internet Model



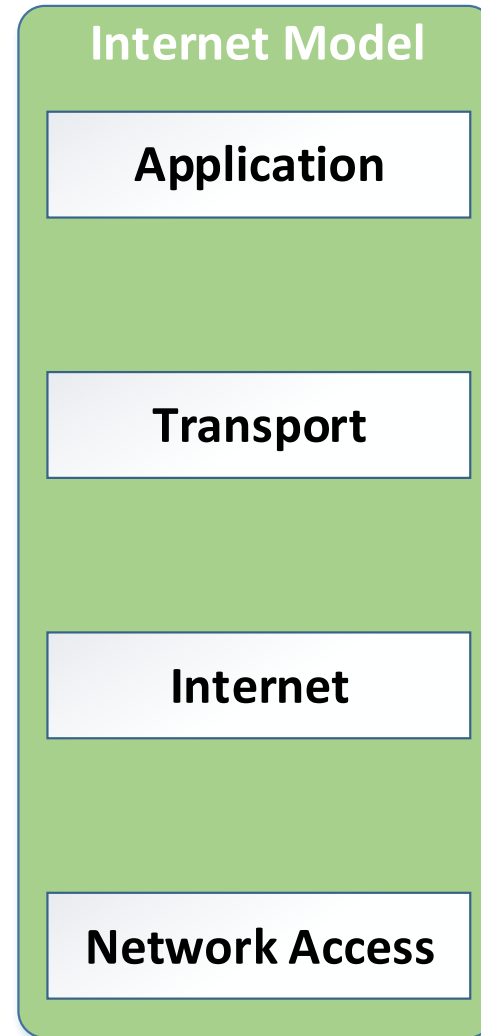
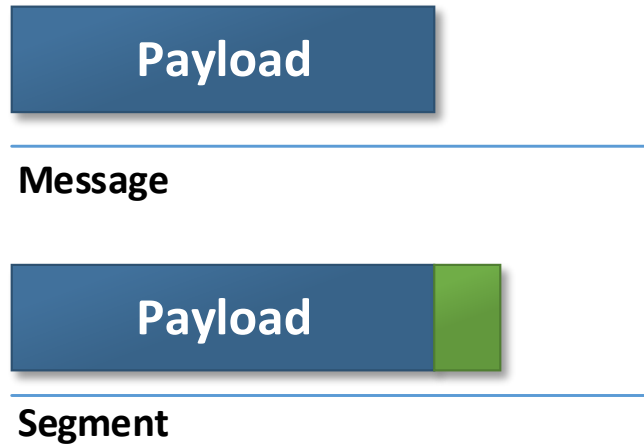
Internet Model

Payload

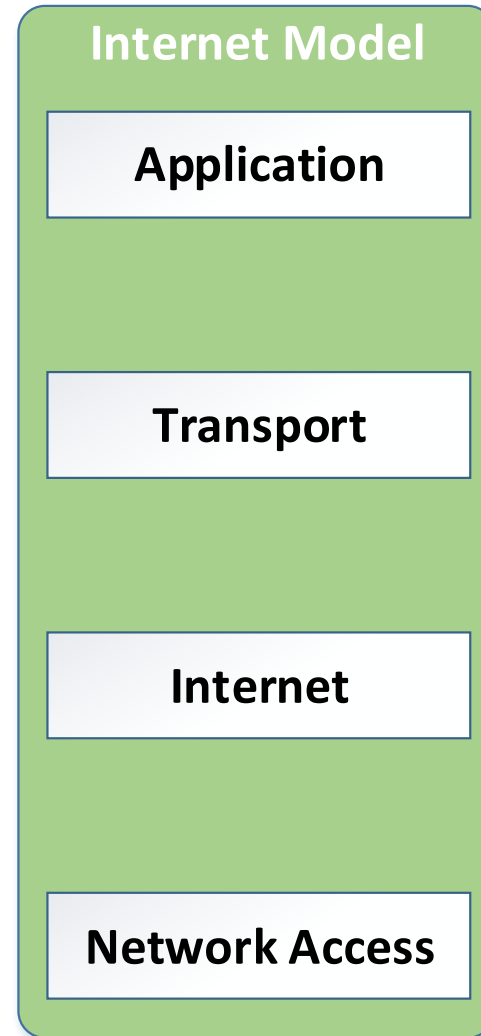
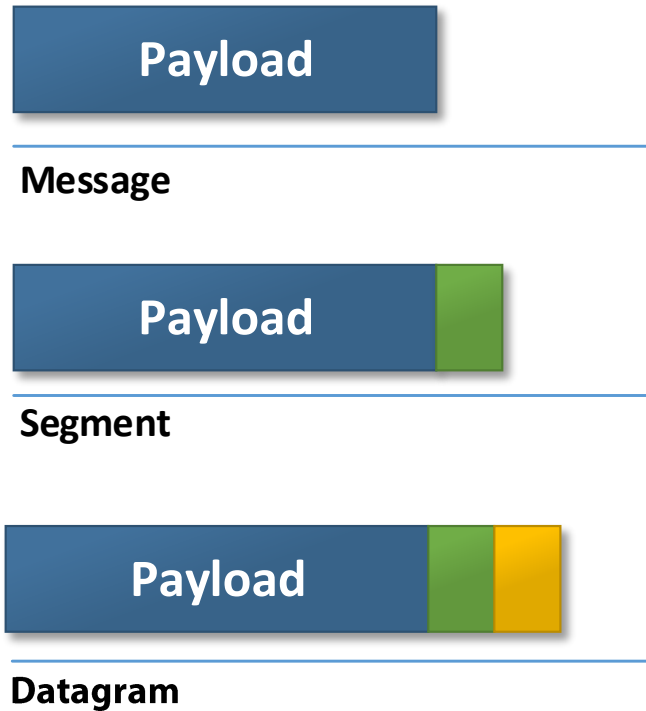
Message



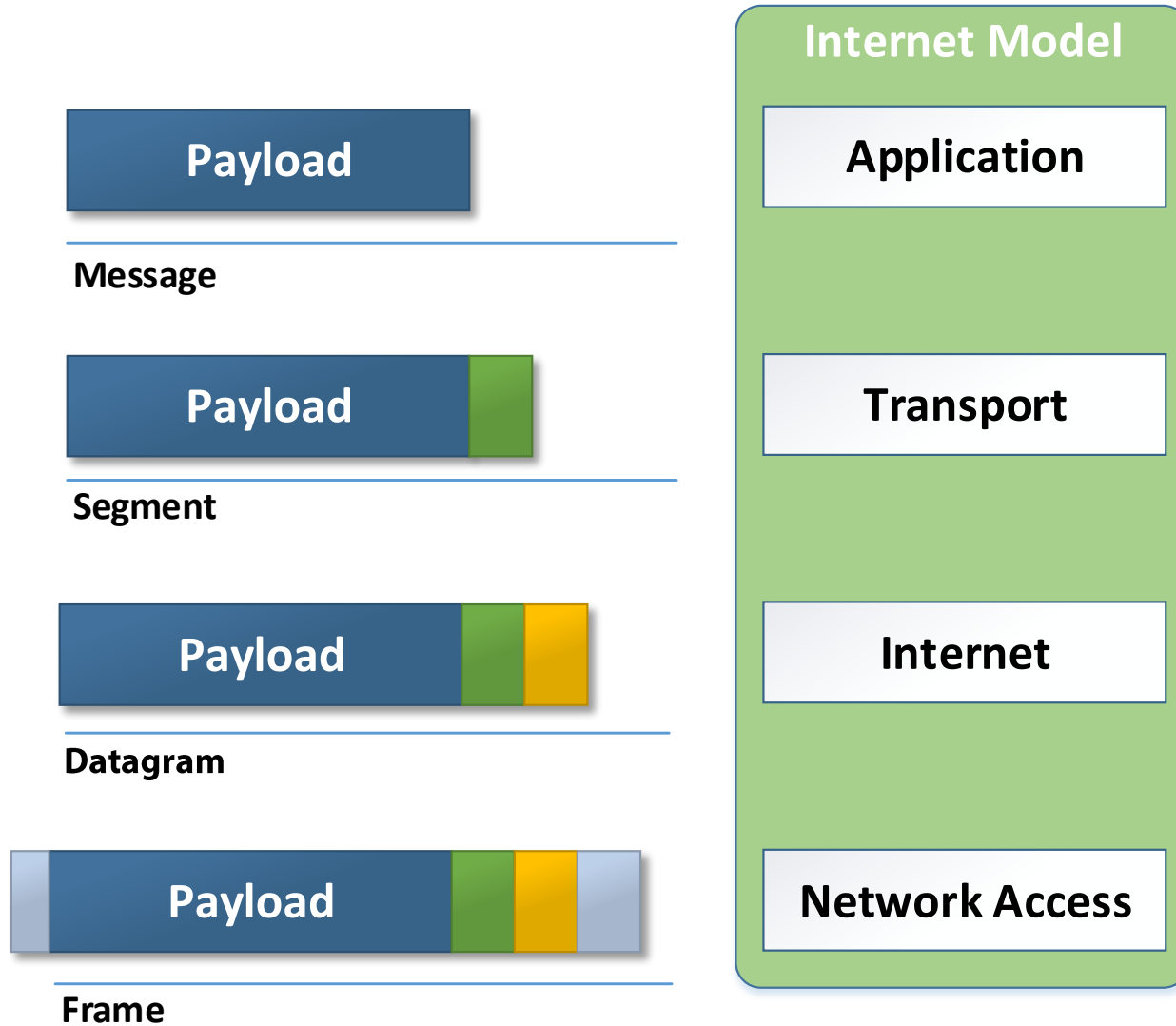
Internet Model



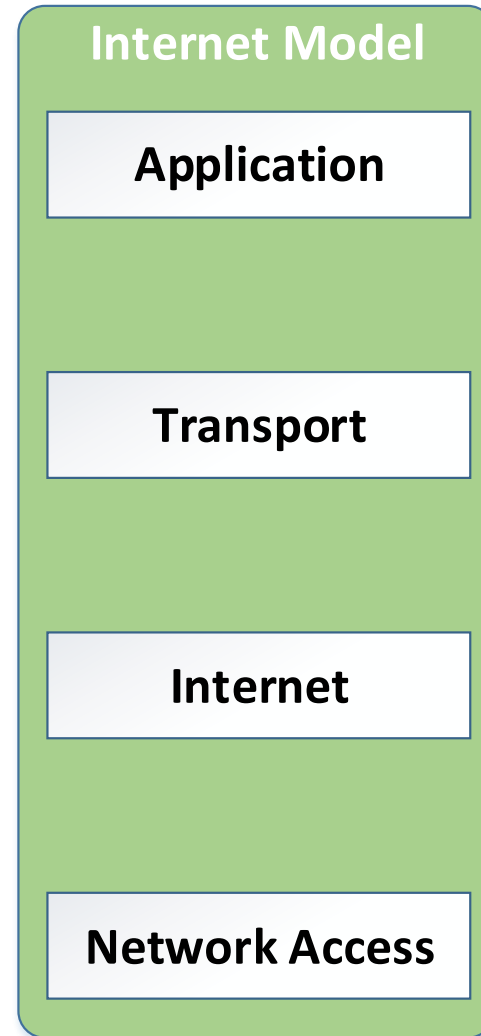
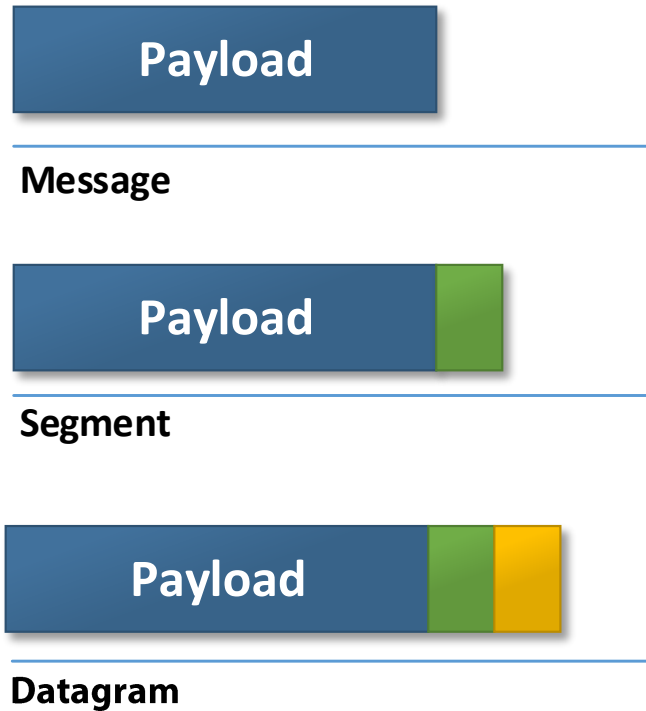
Internet Model



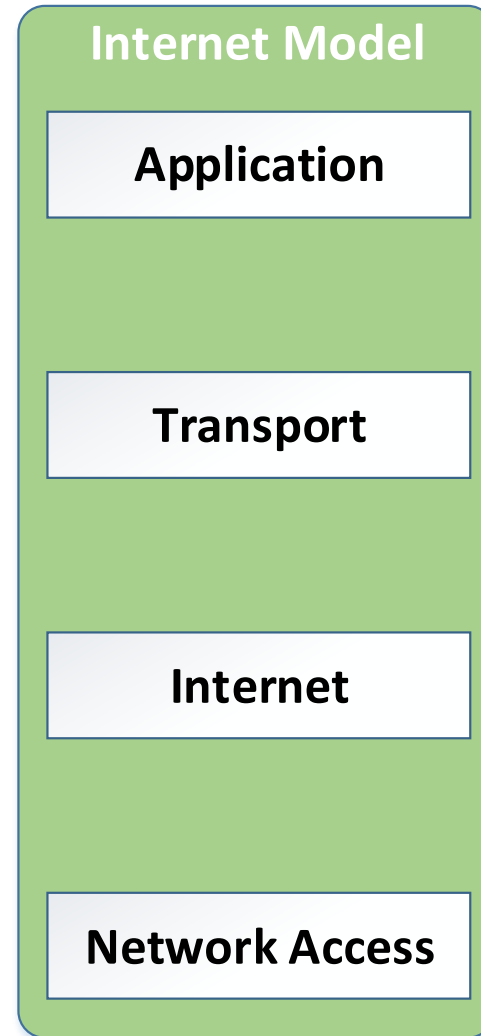
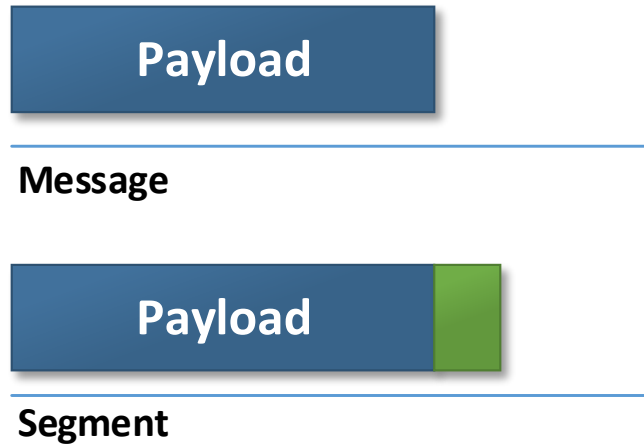
Internet Model



Internet Model



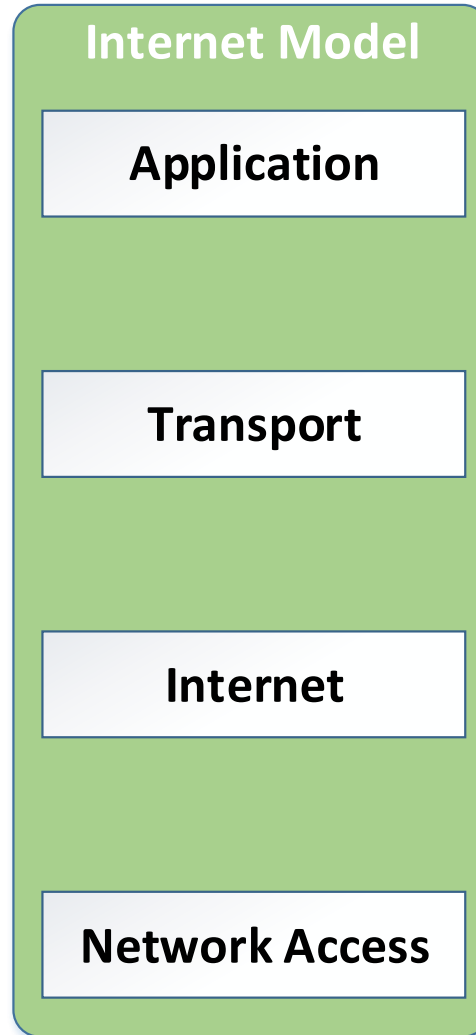
Internet Model



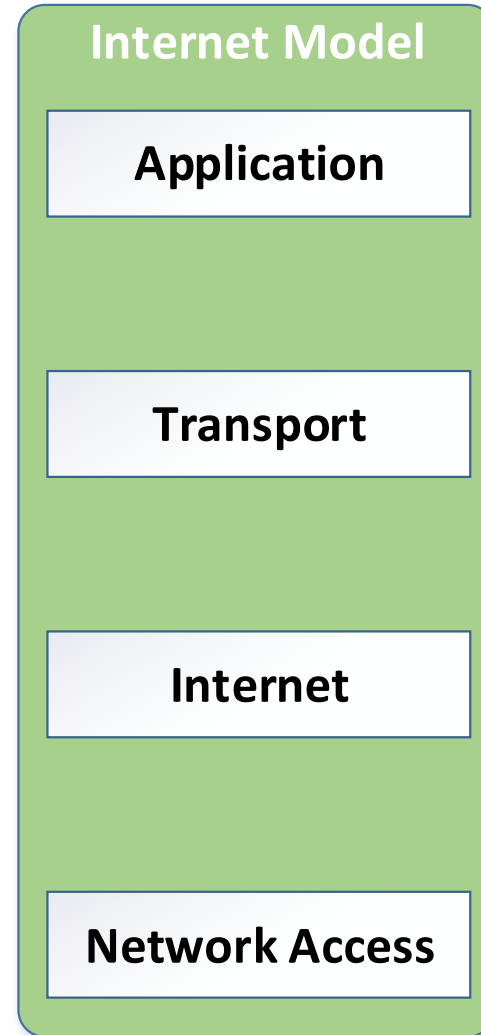
Internet Model

Payload

Message



Internet Model



Networking Protocols

- **IP (Internet Protocol)**

- **Connectionless** protocol
- Responsible for network addressing
- Provides routing of packets between networks

- **TCP (Transmission Control Protocol)**

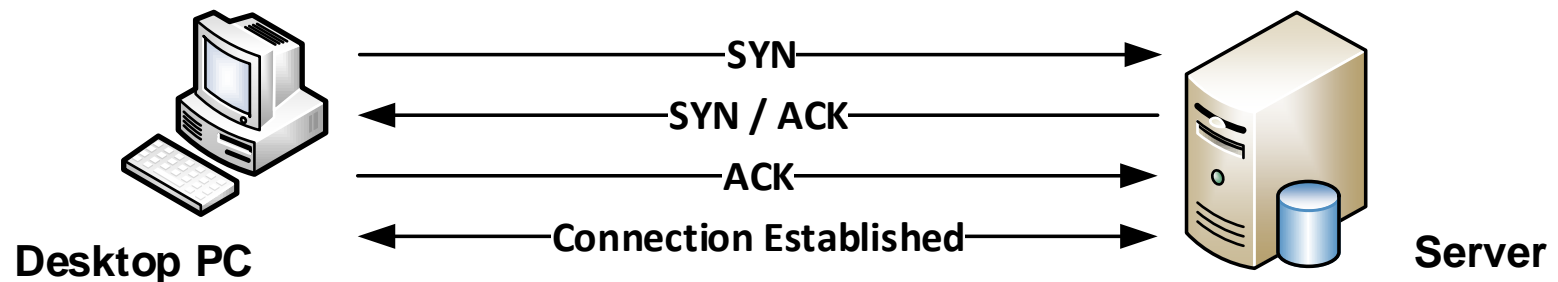
- **Connection** oriented
- Establishes connections between end-points
- Provides guaranteed delivery of packets

- **UDP (User Datagram Protocol)**

- **Connectionless** oriented
- No guarantee of deliver (best effort)

TCP Three-Way Handshake

- Three-way handshake **establishes connection** between two hosts
 - A client node sends a **SYN** data packet over an IP network to a server to determine if the server is open for new connection
 - The target server must have open ports that can accept and initiate new connections. Server responds and returns a confirmation receipt (**SYN/ACK** packet)
 - The client node receives the **SYN/ACK** from the server and responds with an **ACK** packet and establishes a connection



Common **Application Layer** Protocols and Ports

Protocol	Port
FTP	TCP Port 20 & 21
FTPS	TCP Port 989 & 990
SSH and SCP	TCP Port 22
Telnet	TCP Port 23
SMTP	TCP Port 25
DNS	UDP Port 53

Description

- File Transfer Protocol
- Transferring Files from client to server and server to client

Security Considerations

- Insecure (Credentials and transmissions sent in plain text)
- Can be sniffed and used in Man in the Middle or replay attacks

Common **Application Layer** Protocols and Ports

Protocol	Port
FTP	TCP Port 20 & 21
FTPS	TCP Port 989 & 990
SSH and SCP	TCP Port 22
Telnet	TCP Port 23
SMTP	TCP Port 25
DNS	UDP Port 53

Description

- File Transfer Protocol Secure or FTP over SSL
- Secure File Transfer

Security Considerations

- Uses SSL for encryption
- Encryption can be turned off if other encryption is in use

Common **Application Layer** Protocols and Ports

Protocol	Port
FTP	TCP Port 20 & 21
FTPS	TCP Port 989 & 990
SSH and SCP	TCP Port 22
Telnet	TCP Port 23
SMTP	TCP Port 25
DNS	UDP Port 53

Description

- Secure Shell used to securely log into remote devices
- Can be used to add security to other applications

Security Considerations

- Encrypts transmissions and provides integrity checking
- Secure Copy (SCP) uses SSH to securely transfer files (unattended)

Common **Application Layer** Protocols and Ports

Protocol	Port
FTP	TCP Port 20 & 21
FTPS	TCP Port 989 & 990
SSH and SCP	TCP Port 22
Telnet	TCP Port 23
SMTP	TCP Port 25
DNS	UDP Port 53

Description

- Used for remote access and configuration
- Disable if possible

Security Considerations

- Communicates in clear text / no encryption
- Open to traffic sniffers

Common **Application Layer** Protocols and Ports

Protocol	Port
FTP	TCP Port 20 & 21
FTPS	TCP Port 989 & 990
SSH and SCP	TCP Port 22
Telnet	TCP Port 23
SMTP	TCP Port 25
DNS	UDP Port 53

Description

- Simple Mail Transport Protocol
- Email delivery Server to Server
- POP and IMAP moves email from server to client

Security Considerations

- No encryption inherent in the protocol
- Should use S/MIME or PGP for encryption when necessary
- Disable the SMTP open relay feature to limit SPAM and relay attacks

Common **Application Layer** Protocols and Ports

Protocol	Port
FTP	TCP Port 20 & 21
FTPS	TCP Port 989 & 990
SSH and SCP	TCP Port 22
Telnet	TCP Port 23
SMTP	TCP Port 25
DNS	UDP Port 53

Description

- Domain Name System
- Resolves URL to IP address

Security Considerations

- Vulnerable to DNS poisoning
- Can be spoofed in PHISHING attacks

Common **Application Layer** Protocols and Ports

Protocol	Port
TFTP	UDP Port 69
HTTP	TCP Port 80
HTTPS	TCP Port 443
SSL/TLS	
SFTP	TCP Port 115
SNMP	UDP Port 161

Description

- Trivial File Transfer Protocol
- Originally used for network boots and PXE environments

Security Considerations

- No authentication or encryption
- Anonymous connections
- Should be disabled whenever possible

Common **Application Layer** Protocols and Ports

Protocol	Port
TFTP	UDP Port 69
HTTP	TCP Port 80
HTTPS	TCP Port 443
SSL/TLS	
SFTP	TCP Port 115
SNMP	UDP Port 161

Description

- Hypertext Transfer Protocol
- Used to access web pages from web servers

Security Considerations

- No encryption or authentication
- Vulnerable to sniffer, header injection, replay and man in the middle attacks

Common **Application Layer** Protocols and Ports

Protocol	Port
TFTP	UDP Port 69
HTTP	TCP Port 80
HTTPS	TCP Port 443
SSL/TLS	
SFTP	TCP Port 115
SNMP	UDP Port 161

Description

- Hypertext Transfer Protocol Secure or over SSL
- Used for securely accessing web pages
- Uses SSL or TLS for security

Security Considerations

- Only as strong as the TLS or SSL underneath
- Certificates could be compromised
- Heartbleed bug discovered in April 2014 (CVE-2014-0160)

Common **Application Layer** Protocols and Ports

Protocol	Port
TFTP	UDP Port 69
HTTP	TCP Port 80
HTTPS	TCP Port 443
SSL/TLS	
SFTP	TCP Port 115
SNMP	UDP Port 161

Description

- Secure Sockets Layer (SSL) and Transport Layer Security (TLS)
- TLS is newer, based on SSL

Security Considerations

- Adds confidentiality and data integrity by encapsulating other protocols
- Initiates Stateful session with handshake
- Be sure all servers are patched for Heartbleed bug

Common **Application Layer** Protocols and Ports

Protocol	Port
TFTP	UDP Port 69
HTTP	TCP Port 80
HTTPS	TCP Port 443
SSL/TLS	
SFTP	TCP Port 115
SNMP	UDP Port 161

Description

- Secure FTP
- SSH File Transfer Protocol
- Provides remote file transfer, access and management

Security Considerations

- Full server Secure File Transfer
- Distinction: FTP over SSH is FTP tunneled through SSH connection

Common **Application Layer** Protocols and Ports

Protocol	Port
TFTP	UDP Port 69
HTTP	TCP Port 80
HTTPS	TCP Port 443
SSL/TLS	
SFTP	TCP Port 115
SNMP	UDP Port 161

Description

- Simple Network Management Protocol
- Used for remote management and reporting of IP devices

Security Considerations

- v1 and v2 offered no security or encryption
- v3 offers encryption – use whenever possible
- Can be vulnerable to Brute Force and Dictionary attacks

Common **Application Layer** Protocols and Ports

Protocol	Port	Service	NetBIOS Application
NetBIOS	UDP Port 137	Name Service	Redirector
	UDP Port 138	Datagram Service	Messenger
	TCP Port 139	Session Service	Server

Description

- NetBIOS can provide name resolution, connectionless communication (Datagram Service) and Connection-oriented communication (Sessions Service)

Security Considerations

- Vulnerable to NetBIOS Name Service spoofing (NBNS Spoofing)
- Disable if not needed

Common **Transport Layer** Protocols and Ports

Protocol	Description
TCP	Transmission Control Protocol
UDP	User Datagram Protocol

Description

- Transmission Control Protocol
- Provides session service to the application layer
- Three-way handshake to establish connection

Security Considerations

- Vulnerable to TCP/IP Hijacking, sequence number attack and SYN flood attacks

Common **Transport Layer** Protocols and Ports

Protocol	Description
TCP	Transmission Control Protocol
UDP	User Datagram Protocol

Description

- User Datagram Protocol
- Provides datagram service to the application layer

Security Considerations

- Connectionless (but faster than TCP)
- No error checking
- Vulnerable to UDP flooding attacks

Common **Internet Layer** Protocols and Ports

Protocol	Description
IPv4 / IPv6	IPv4 (32-bit Address) / IPv6 is 128-bit address
ICMP	Internet Control Message Protocol
ARP/RARP	Address Resolution Protocol / Reverse ARP

IPv4 Address: **192.168.110.235**

IPv6 Address: **FE80:22:35:12:1215:4325:0:120**

Description

- Internet Protocol
- Used for addressing and routing

Security Considerations

- Does not verify message accuracy (TCP handles)
- IPv6 has IPsec built-in

Common **Internet Layer** Protocols and Ports

Protocol	Description
IPv4 / IPv6	IPv4 (32-bit Address) / IPv6 is 128-bit address
ICMP	Internet Control Message Protocol
ARP/RARP	Address Resolution Protocol / Reverse ARP

- Echo Reply and Echo Request
- Source Quench
- Router Advertisement Reply and Router Solicitation
- Destination Unreachable
- Redirect
- Time Exceeded

```
C:\Users\cdr>ping 10.1.10.1

Pinging 10.1.10.1 with 32 bytes of data:
Reply from 10.1.10.1: bytes=32 time<1ms TTL=64
Reply from 10.1.10.1: bytes=32 time<1ms TTL=64
Reply from 10.1.10.1: bytes=32 time<1ms TTL=64
Reply from 10.1.10.1: bytes=32 time<1ms TTL=64

Ping statistics for 10.1.10.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
```


Common **Internet Layer** Protocols and Ports

Protocol	Description
IPv4 / IPv6	IPv4 (32-bit Address) / IPv6 is 128-bit address
ICMP	Internet Control Message Protocol
ARP/RARP	Address Resolution Protocol / Reverse ARP

```
C:\Users\cdr>arp -a

Interface: 10.1.10.101 --- 0xa
 Internet Address      Physical Address      Type
 10.1.10.1             c4-04-15-ba-60-4c     dynamic
 10.1.10.100           20-aa-4b-a6-7c-8f     dynamic
 10.1.10.101           08-00-27-1d-47-b6     dynamic
```

Description

- Translates IP address to MAC address

Security Considerations

- No authentication
- Vulnerable to ARP spoofing (also called ARP cache poisoning)
 - Can be used for Man in the Middle attacks

SAN Protocols

- **Fibre Channel (FCP)**

- Transports **SCSI** commands over Fibre Channel Networks
- 2, 4, 8 and 16Gbps speeds
- Hosts have Host Bus Adapters(HBA) similar to NICs in IP Networks
 - HBA has a **WWN** (World-Wide Name) similar to MAC address that is unique
 - WWPN – Port WWN (unique per port)
 - WWNN – Node WWN (shared by some or all ports on a device)

SAN Protocols

- **Fibre Channel (FCP)**
 - Switches are used to connect hosts to storage arrays
 - Switches – Fixed configuration (sometimes semi-modular)
 - Directors – Modular with high port count and high availability



Cisco MDS 9250i



Cisco MDS 9710

SAN Storage

SAN Storage Array (**Multiple** Engines, **Thousands** of Disk Drives)



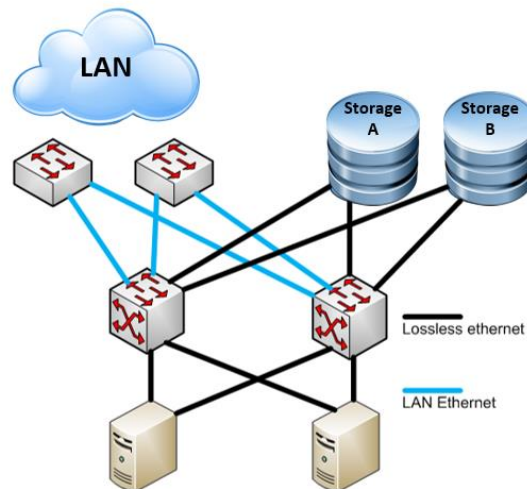
SAN Protocols

■ iSCSI

- Enables SCSI commands to be sent over an **IP network**
- Alternative to dedicated Fibre Channel cabling
 - Should have dedicated subnets or VLANs to avoid resource contention

■ FCoE

- Alternative to Fibre Channel
- Runs on top of Ethernet in the protocol stack (iSCSI runs on top of IP)
 - Not routable



Well Known Ports

- 21 – FTP
- 22 – SSH / SCP / SFTP
- 25 – SMTP
- 53 – DNS
- 80 – HTTP
- 110 – POP3
- 139 – NetBIOS
- 143 – IMAP
- 443 – HTTPS (TLS/SSL)
- 3389 – Remote Desktop Protocol (RDP)

Protocols and Ports Review

- IPsec
- SNMP
- SSH
- DNS
- TLS
- SSL
- TCP/IP
- FTPS
- HTTPS
- SCP
- ICMP
- IPv4
- IPv6
- iSCSI
- Fibre Channel
- FCoE
- FTP
- SFTP
- TFTP
- TELNET
- HTTP
- NetBIOS



From a **security perspective**, understand what protocols are **secure**, and which ones **aren't**.

- Disable or block insecure protocols
- Use encryption when possible (over insecure networks)