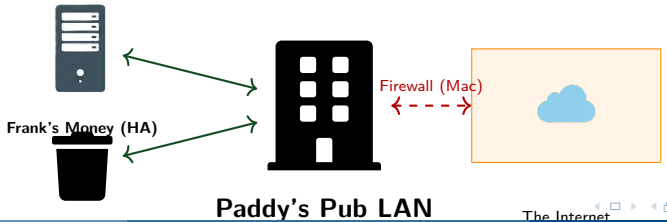
Module 7.0: Network Services & High Availability

"The Gang Configures the Network"

Brendan Shea, PhD

Rochester Community and Technical College



Outline I

Review: The Gang Recaps Module 6

Previous Concepts

- **TCP/UDP**: Transport protocols. Reliable (TCP) vs Fast (UDP).
- **DHCP**: Dynamic Host Configuration Protocol. Assigns IPs.
- **DNS**: Domain Name System. Resolves names.

The New Problem

We have connectivity, but...

- Is the connection secure? (Can the McPoyles spy on us?)
- Is the time synced? (Are we opening on time?)
- Is the data backed up? (What if Dennis burns it down?)

Learning Outcomes I

After completing this module, you will be able to:

- Explain how **TLS** (Transport Layer Security) provides encryption, authentication, and integrity for secure communication.
- Describe the role of **NTP** (Network Time Protocol) in synchronizing system clocks across distributed networks and explain its importance for security and logging.
- Compare **HTTP** and **HTTPS** for web services, and explain how **FTP**, **FTPS**, and **SFTP** are used for file transfer.
- Explain the **SMB/CIFS** protocol for Windows file sharing and how **SAN** (Storage Area Network) and **NAS** (Network Attached Storage) differ.
- Describe email protocols: **SMTP** (sending), **POP3** (mailbox download), and **IMAP** (synchronized access).
- Explain **VoIP** (Voice over IP) components including **H.323**, **SIP**, and **RTP**, and identify QoS requirements for voice traffic.

Learning Outcomes II

- Describe **RAID** levels (0, 1, 5, 6, 10) for disk redundancy and explain trade-offs between performance, capacity, and fault tolerance.
- Explain **clustering** for server redundancy and identify **FHRP** protocols (HSRP, VRRP, GLBP) for router/gateway high availability.
- Define **RTO** (Recovery Time Objective) and **RPO** (Recovery Point Objective) for disaster recovery planning.
- Compare backup strategies (full, incremental, differential) and explain offsite replication and **hot/warm/cold sites** for business continuity.

Section 7.1: Security and Time (Charlie Work)

"The Gang Secures the Network"

cue music...

Core Concepts

- **TLS**: Transport Layer Security. Encrypts traffic (e.g., HTTPS).
- **NTP**: Network Time Protocol. Syncs clocks for logs and auth.

TLS: Transport Layer Security

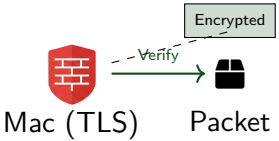
Definition

TLS is a cryptographic protocol designed to provide:

1. **Encryption**: Privacy (No eavesdropping).
2. **Integrity**: Data has not been changed.
3. **Authentication**: Verifying identity.

Analogy: Mac's "Ocular Patdown"

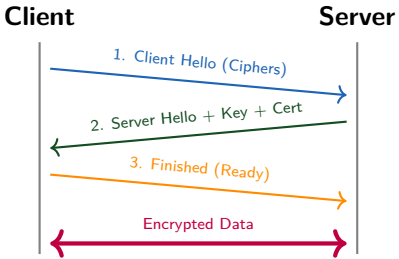
Mac assesses a threat (Authentication), ensures they aren't carrying weapons (Integrity), and clears them for entry.



Warning

SSL is insecure. Always use **TLS 1.2** or **1.3**.

TLS 1.3 Handshake: The Process



Technical Steps

1. **Client Hello**: "I speak these ciphers."
2. **Server Hello**: "Use this one. Here is my Cert."
3. **Key Exchange**: Generating session keys.
4. **Finished**: Secure tunnel up.

Analogy

The "Secret Handshake" before the gang discusses the scheme.

Certificates and Trust

Digital Certificates (X.509)

Binds an identity (Domain Name) to a Public Key.

- **CA (Certificate Authority)**: Trusted 3rd party.
- **Chain of Trust**: Root CA -> Intermediate -> Server Cert.

Self-Signed Certificates

Signed by itself, not a trusted CA.

- **Result:** Browser warning ("Not Secure").
- **Use Case:** Internal testing only.

Analogy: Bird Law

A Certificate is a contract. You need a Judge (CA) to enforce it. Charlie's "Bird Law" (Self-Signed) is not recognized in court.

NTP: Network Time Protocol

Definition

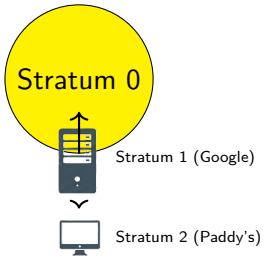
Protocol used to synchronize clocks.

- **Port**: UDP 123.
- **Why?**: Log correlation, Auth (Kerberos), Backups.

Stratum Levels

Hierarchy of distance from source.

- **Stratum 0**: Atomic Clock (The Source).
- **Stratum 1**: Directly connected to S0.
- **Stratum 16**: Unsynchronized (Desync).



Analogy: Charlie Work

Charlie ensures all clocks match so the bar opens exactly at 11 AM.

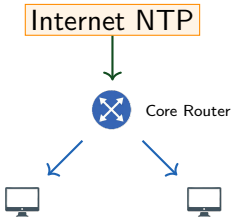
NTP Architecture: Hierarchy

Best Practice Setup

Don't have every PC query the internet.

1. **Router** queries Public NTP (pool.ntp.org).
2. **Switch** queries Router.
3. **PC/Server** queries Switch/Router.

This creates a single internal time source.



Precision Time Protocol (PTP)

When Milliseconds Aren't Good Enough

NTP is accurate to milliseconds (ms). **PTP (IEEE 1588)** is accurate to **microseconds (μs)** or even nanoseconds.

Use Cases

- **5G**: Cellular Sync.
- **Finance**: High-frequency trading.
- **Automation**: Robotics.

Analogy: The Nightman Cometh

In a musical, lights and audio must sync perfectly. Being off by 1ms ruins the show.

Case Study: Dennis & The Paddy's Time Heist

▶ Case Study: "The Gang's POS System Fails"

Paddy's POS system is rejecting credit cards with error: **"Certificate not yet valid."**

Facts:

- Current Date: June 1, 2025.
- System Date: **Jan 15, 1970** (Mac unplugged it).
- Cert Valid From: Jan 1, 2024.

"The computer thinks the internet hasn't been invented yet!" - Charlie

Review Questions

1. Why does the wrong date break TLS?
2. What protocol is missing?
3. How do we fix it permanently?

Case Study Solution: The Paddy's Time Heist

✓ Solution: "The Gang Learns About Time"

1. **Validity**: The system thinks it is 1970. The certificate (from 2024) is "from the future" and thus invalid.
2. **Protocol**: **NTP** (Network Time Protocol).
3. **Fix**: Configure the POS to sync with `pool.ntp.org`.

The Fix

```
# chrony.conf
server 0.pool.ntp.org iburst
```

Lesson

If time is broken, **Security is broken**. (Logs, Auth, and Certs all fail).

Section 7.2: Web and File Services (Dennis's Domain)

"The Gang Goes Online"

What we will cover

- **Web Browsing**: How Chrome talks to Servers (HTTP/HTTPS).
- **File Transfer**: Moving files across the internet (FTP).
- **File Sharing**: Accessing folders on the office network (SMB).
- **Storage**: Where the data actually lives (NAS/SAN/DB).

HTTP: Hypertext Transfer Protocol

What is it?

The language web browsers use to request webpages.

- **Port**: TCP 80.
- **Nature**: **Cleartext** (Not encrypted).

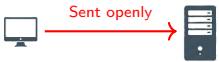
Analogy: Shouting in the Bar

If Charlie shouts "What is the Wi-Fi password?" across the bar, **everyone** hears it.

- **Client**: Charlie (Browser).
- **Server**: Dennis (Web Server).
- **Risk**: Frank (Hacker) is listening.

The Conversation (Request/Response)

```
Browser (GET):
GET /menu.html HTTP/1.1
Host:  www.paddyspub.com
Server (Response):
HTTP/1.1 200 OK
Content-Type:  text/html
<html><body><h1>Wolf Cola</h1>...
```



HTTPS: HTTP Secure

What is it?

HTTP inside a secure, encrypted tunnel (TLS).

- **Port**: TCP 443.
- **Security**: Encrypted (Scrambled).
- **Indicator**: The 🔒 Lock icon in Chrome.

Analogy: The Back Office

Dennis takes the customer into the back office and locks the door to discuss "business."

- Frank can see them go in, but he **cannot hear** what they are saying.

HSTS

HTTP Strict Transport Security: A rule servers send to browsers saying "Never talk to me on Port 80 again. Only use Port 443."

HTTP Versions: Evolution of Speed

Why do we keep changing it?

The internet got heavier (images, videos). We needed faster ways to load pages.

HTTP/1.1 (1997)

"One at a time."

- Load image 1. Wait.
- Load image 2. Wait.
- **Slow.**

HTTP/2 (2015)

"Multiplexing."

- Load 10 images at once over one connection.
- Like carrying 10 beers on a tray.

HTTP/3 (2022)

"QUIC (UDP)."

- Abandon TCP!
- Uses UDP for raw speed.
- Fast setup (0-RTT).

FTP: File Transfer Protocol

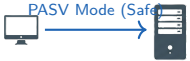
What is it?

A protocol specifically for uploading/downloading files.

- **Port 21**: Control (Commands like "List files").
- **Port 20**: Data (The actual file content).

Active vs. Passive

- **Active Mode**: The Server tries to connect back to the Client. *Firewalls block this ("Who is this server calling me?").*
- **Passive Mode (PASV)**: The Client connects to the Server. *Firewalls like this (Client initiated it).*



The Problem

FTP sends your **Username and Password** in plain text! *If Frank is sniffing the network, he gets your password immediately.*

Secure File Transfer: Don't use FTP!

SFTP (SSH File Transfer)

Recommended Standard.

- **Port**: TCP 22 (Same as SSH).
- **How**: It runs inside an SSH tunnel.
- **Pros**: Only 1 port to open on the firewall.

FTPS (FTP over SSL)

The Old Way.

- **Ports**: 989/990.
- **How**: Standard FTP wrapped in a certificate.
- **Cons**: Still uses multiple ports (Control/Data). Hard to firewall.

Exam Tip

If you see **SFTP**, think **SSH** (Port 22). If you see **FTPS**, think **SSL** (Certificates).

SMB: Server Message Block

What is it?

Windows File Sharing. This is what you use when you access a "Shared Folder" on the office network.

- **Port**: TCP 445.
- **Example**: `\\PaddysServer\Schemes`.
- **Mapping**: "The Z: Drive".

Security Warning: SMBv1

SMB Version 1 is extremely dangerous.

- It contains the **EternalBlue** vulnerability.
- This allowed the **WannaCry Ransomware** to spread worldwide in 2017.
- **Fix**: Disable SMBv1 on all Windows computers immediately.

Storage: NAS vs. SAN

Where does the data live?

When the server's hard drive is full, we buy dedicated storage.

NAS (Network Attached Storage)

"The Shared Box"

- **Type**: File Level.
- **Connection**: Ethernet (plug it into the switch).
- **Analogy**: A digital filing cabinet everyone can open.
- **Best for**: Office docs, backups.

SAN (Storage Area Network)

"The Virtual Disk"

- **Type**: Block Level.
- **Connection**: Fiber Channel (Expensive cables).
- **Analogy**: A hard drive attached via a very long cable. The server thinks it's a local disk.
- **Best for**: High-speed databases.

NAS Use Case: "The Evidence Locker"

Scenario

Dennis needs a place to store his... "videotapes."

1. He buys a Synology NAS.
2. He plugs it into the Paddy's Switch.
3. He creates a shared folder: `\\NAS\Evidence`.
4. He sets permissions so only he can delete files.

RAID (Redundancy)

Dennis uses **RAID 1** (Mirroring) inside the NAS.

- If Drive A fails, Drive B still has the data.
- *"Two is one, and one is none."*

Synology NAS

Databases: Frank's "Cooked Books"

SQL (Relational)

Structured Tables. Like an Excel sheet with strict rules.

- **Examples**: MySQL (port 3306), Microsoft SQL Server (port 1433).
- **Use**: Financial records, Inventory.
- **Frank's Query**: `SELECT * FROM Taxes WHERE Paid = 'False'`

NoSQL (Non-Relational)

Unstructured Data. Like a box of receipts.

- **Examples**: MongoDB, Redis.
- **Use**: Social media posts, caching, rapid data.
- **Benefit**: Very fast, flexible structure.

Security

Never expose your database port (e.g., 3306) to the internet. Hackers will brute-force the password in seconds. Keep it behind the firewall!

Case Study: Charlie's Rat Removal Website

▶ Case Study: "The Gang Gets Hacked"

Charlie launches `charliesratremoval.com` (Port 80). He collects credit card payments for his services. It works fine when he tests it locally. However:

- **Problem**: Customers see a red **"NOT SECURE"** warning.
- **Observation**: Frank intercepts credit card numbers in cleartext using Wireshark.

Discussion

1. Why was Frank able to steal the data?
2. What port/protocol must Charlie enable?
3. What does Charlie need to install?

Case Study Solution: Charlie's Rat Removal

✓ Solution: "The Gang Encrypts"

1. **Vulnerability**: HTTP (Port 80) sends data in **Cleartext**.
2. **Fix**: Enable **HTTPS** on Port 443.
3. **Requirement**: A **TLS Certificate** (e.g., Let's Encrypt).

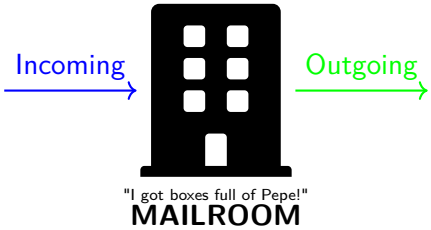
The Fix

```
$ sudo apt install certbot
$ sudo certbot -apache
```

Result

Frank opens Wireshark again. He only sees encrypted garbage.

Section 7.3: Email & Voice (The Conspiracy)



Agents

- **MUA**: User Agent (Outlook, Thunderbird, Apple Mail).
- **MTA**: Transfer Agent (SMTP Server).
- **MDA**: Delivery Agent (IMAP/POP3 Server).

Protocols

- **SMTP**: Sending.
- **IMAP/POP3**: Receiving.

SMTP: Simple Mail Transfer Protocol

Sending Mail

SMTP is a **Push** protocol.

- **Port 25**: Server-to-Server. Shouldn't be used by clients, since it isn't secured.
- **Port 587**: Client-to-Server. Secured with TLS.
- **Port 465**: SMTP over SSL (Deprecated).

The Conversation

```
S: 220 paddys.com ESMTP
C: HELO google.com
S: 250 Hello
C: MAIL FROM: <dee@paddys.com>
C: RCPT TO: <waitress@coffee.com>
C: DATA
C: Subject:  Bird
C: .
S: 250 Ok:  queued
```

Spam Prevention

Use **SPF, DKIM, DMARC** to prove identity. These prevent spoofing by using DNS records and cryptographic signatures.

Receiving Mail: IMAP vs. POP3

IMAP (Sync)

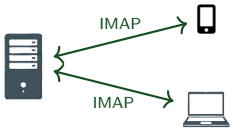
"The Cloud" (143/993)

- Stays on server.
- Synced on all devices.
- **Best for:** Dee, since she checks mail on phone & PC. (Multi-device).

POP3 (Download)

"Local Only" (110/995)

- Download & Delete.
- Local storage only.
- **Best for:** Frank, who only checks mail on one PC. (Single-device). He can free up server space, and archive locally.



VoIP: Voice Over IP (The Gang Starts a Call Center)

What is VoIP?

Sending voice as UDP packets.

- **Unified Comms**: Video/Voice/Chat.
- **Hard Phone**: Desk phone.
- **Soft Phone**: App (Teams).

Bandwidth

Codec	**Speed**	
G.711	64 Kbps	*Streaming 4K video kills*
G.729	8 Kbps	

VoIP (Jitter).

VoIP Protocols: SIP vs. RTP

SIP (Session Initiation)

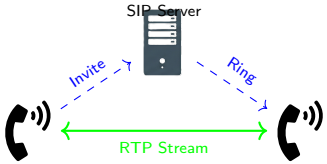
"The Setup" (5060/5061).

- Dialing/Ringing.
- "Hello?" / "Goodbye."

RTP (Real-time Transport)

"The Stream" (UDP).

- The actual audio data.
- Flows directly between phones.



VoIP Infrastructure: Power and VLANs

PoE (Power over Ethernet)

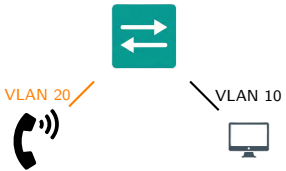
Sends power down the cable.

- **802.3af**: 15.4W.
- **802.3at**: 30W (Video).

Voice VLANs

- **VLAN 20**: Phones.
- **VLAN 10**: PCs.
- **Benefit**: Security + QoS.

PoE Switch



Case Study: The Gang's Call Center

▶ Case Study: "Dee Sounds Like a Robot"

The Gang installs a cheap VoIP system to sell "Wolf Cola."

- **Setup**: IP Phones plugged into the same switch as Mac's gaming PC.
- **Issue**: When Mac downloads game updates, Dee's sales calls start stuttering and dropping.
- **Frank's Reaction**: "I'm not paying for this garbage! Fix it!"

Discussion Questions

1. What network phenomenon is causing the stuttering?
2. Why does Mac's download affect the phones?
3. What technology allows voice to skip the line?

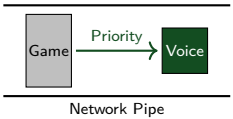
Case Study Solution: The Gang's Call Center

✓ Solution: "The Gang Learns QoS"

1. **Issue**: **Jitter** (Latency variation). Real-time voice cannot tolerate delays.
2. **Cause**: **Congestion**. Mac is filling the bandwidth pipe, forcing voice packets to wait in the buffer.
3. **Fix**: Voice and video traffic should be on a separate VLAN. The voice VLAN should implement **QoS (Quality of Service)** to ensure it has higher priority than best-effort traffic (like game downloads).

QoS Configuration

- **Tagging**: Mark voice packets with **DSCP EF (46)** (Expedited Forwarding).
- **Queuing**: Give EF packets strict priority over Best Effort (Game data).



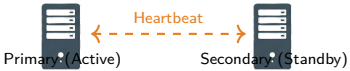
High Availability: "The Show Must Go On"

Concepts

- **HA (High Availability)**: Redundancy to prevent downtime.
- **DR (Disaster Recovery)**: Plan for restoring after a catastrophe.

Availability Metrics

Target	Downtime/Year
99%	3.65 days
99.9%	8.76 hours
99.999%	5 minutes



If Primary dies,
Secondary takes over!

DR Metrics: RTO vs. RPO

How much does Frank lose?

When the server crashes, two clocks start ticking.

RPO (Recovery Point)

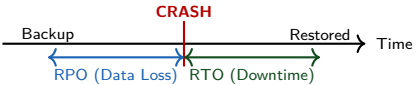
"Data Loss Tolerance"

- How far back do we go?
- If backup was 24h ago, we lost 24h of data.
- *Frank: "Zero!"*

RTO (Recovery Time)

"Downtime Tolerance"

- How long until we are back up?
- Includes repair and restore time.
- *Frank: "Now!"*



DR Sites: Paddy's Pub 2 (Electric Boogaloo)

Cold Site

"Empty Warehouse"

- Power/Net only.
- No hardware.
- **Slowest** / Cheapest.

Warm Site

"Storage Unit"

- Racks ready.
- Restore data needed.
- **Medium** cost.

Hot Site

"The Franchise"

- Exact Mirror.
- Instant failover.
- **Fastest** / Expensive.


Cold


Warm


Hot

Fault Tolerance: RAID

RAID (Redundant Array of Independent Disks) combines multiple physical drives into one logical unit for redundancy and/or performance.

RAID 0 (Striping)

"Charlie Special"

- Fast access.
- **Zero Redundancy**.
- 1 Drive fails = All data lost.

RAID 1 (Mirroring)

"Dennis System"

- Exact duplicate.
- 1 Drive fails = System stays up.
- 50% Capacity cost.

RAID 5 (Parity)

"The Gang Share"

- Data + Parity striped.
- Survives 1 failure.
- Efficient storage.

Parity protects data

FHRP: First Hop Redundancy Protocols

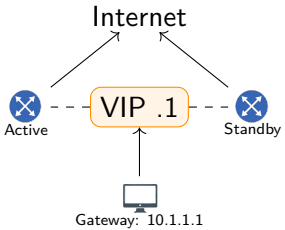
The Problem

If the main router (Gateway) dies, the bar loses internet.

The Solution: Virtual IP

Two routers share ONE IP address.

- **HSRP**: Cisco (Active/Standby).
- **VRRP**: Open (Master/Backup).
- **GLBP**: Load Balancing.



Case Study: Frank's "Foolproof" Plan

▶ Case Study: "The Gang Needs 5 Nines"

Frank demands **99.999%** availability for his gambling ring.

Current Setup:

- Single Consumer Router.
- Charlie manually backing up files to a USB stick "when he remembers."

Frank's Budget: $50.

Discussion

1. Is "Five Nines" realistic?
2. Identify the **SPOF** (Single Point of Failure).
3. Suggest a realistic fix.

Solution: The "Good Enough" Plan

✓ Solution: "Frank Compromises"

1. **Reality Check**: 99.999% costs thousands (redundant ISPs, generators).
2. **SPOF**: The router, the power, and Charlie.
3. **Realistic Fix**:
   - Buy a **UPS (Battery)** for power outages.
   - Automate backups to the **Cloud** (removes Charlie error).

Module 7.0 Summary I

Key Concepts:

- **TLS** (Transport Layer Security): Provides encryption, authentication, and message integrity for secure communication (HTTPS, FTPS).
- **NTP** (Network Time Protocol): Synchronizes system clocks across networks using Stratum hierarchy (0 = reference clock, 15 max). Critical for logging, Kerberos, certificates.
- **HTTP** (Port 80): Unencrypted web traffic. **HTTPS** (Port 443): HTTP over TLS for secure web browsing.
- **FTP** (Ports 20/21): File Transfer Protocol. **FTPS**: FTP over TLS. **SFTP**: SSH File Transfer (Port 22, more secure).
- **SMB/CIFS**: Windows file sharing protocol. Use with **SAN** (Storage Area Network, block-level) or **NAS** (Network Attached Storage, file-level).
- Email: **SMTP** (Port 25/587) sends mail. **POP3** (Port 110) downloads and deletes. **IMAP** (Port 143) keeps synchronized folders.

Module 7.0 Summary II

- **VoIP**: Voice over IP using **H.323** or **SIP** for signaling, **RTP** for media. Requires low latency/jitter (QoS, traffic shaping).

Module 7.0 Summary III

High Availability & Disaster Recovery:

- **RAID**: Disk redundancy. RAID 0 (striping, no redundancy), RAID 1 (mirroring), RAID 5 (striping + parity), RAID 6 (dual parity), RAID 10 (mirroring + striping).
- **Clustering**: Server redundancy (active-active or active-passive). **FHRP**: First Hop Redundancy Protocol (HSRP, VRRP, GLBP) for router/gateway failover.
- **RTO** (Recovery Time Objective): Maximum downtime acceptable. **RPO** (Recovery Point Objective): Maximum data loss acceptable.
- Backups: Full (complete copy), Incremental (changes since last backup), Differential (changes since last full). Use offsite replication for disaster recovery.
- Sites: **Hot site** (fully operational standby), **Warm site** (partial setup), **Cold site** (empty facility, slowest recovery).