Layer 7 Protocols

DOMAIN 1.0

MODULE 4

Layer 7 Protocols Topics

Remote Control Protocols

File Sharing Protocols

Web Protocols

Email Protocols

Database Protocols

Voice Protocols

Security Protocols

Management Protocols

Remote Control Protocols

Remote Desktop Protocol (RDP)

Used to interact with the desktop of a remote computer

Chosen by Microsoft for its Terminal Services

Has a client and server component

- Third party apps for non-Microsoft clients

Client sends keystrokes and mouse clicks to server

Server sends back screen video

Computing actually happens on the server

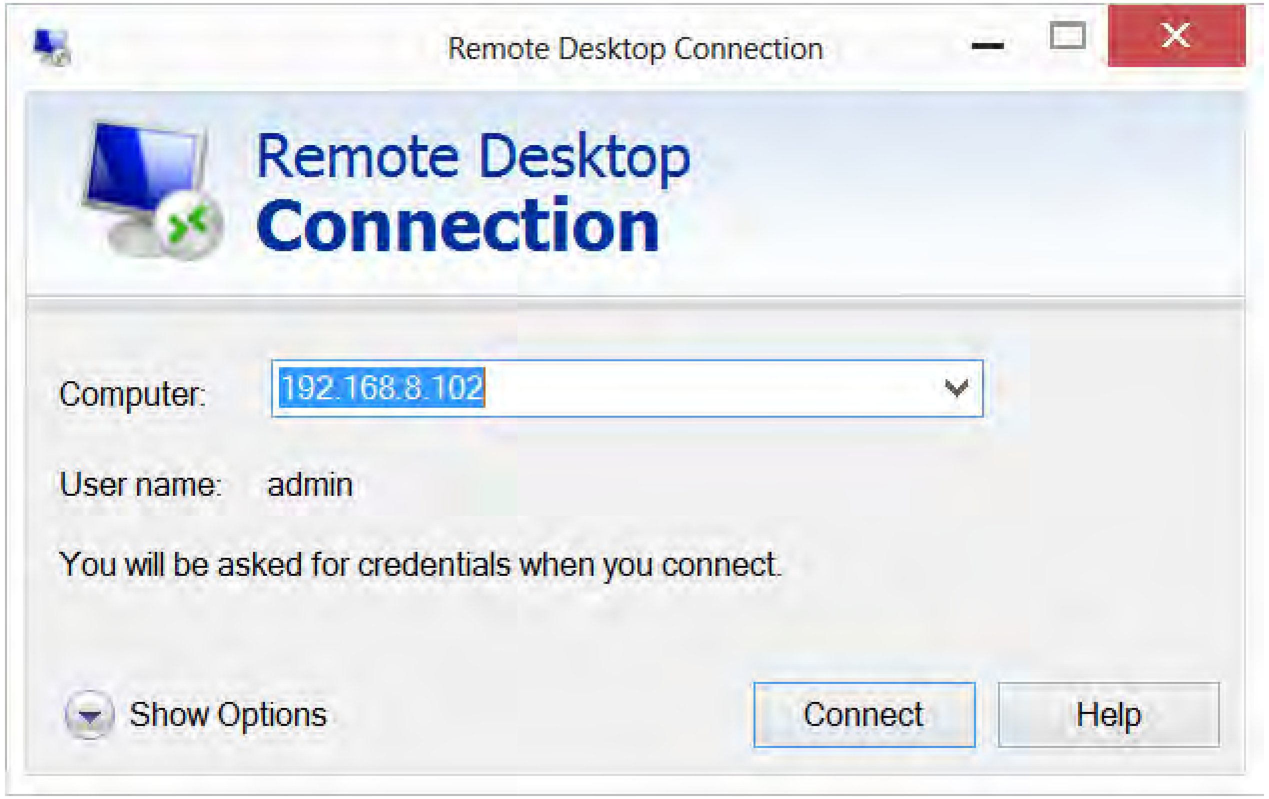
Printer, speakers, drives, and file shares can be mapped between the client and server

TCP 3389 (configurable)

You have different choices for encryption and compression

RDP Login Screen

Client app name = mstsc

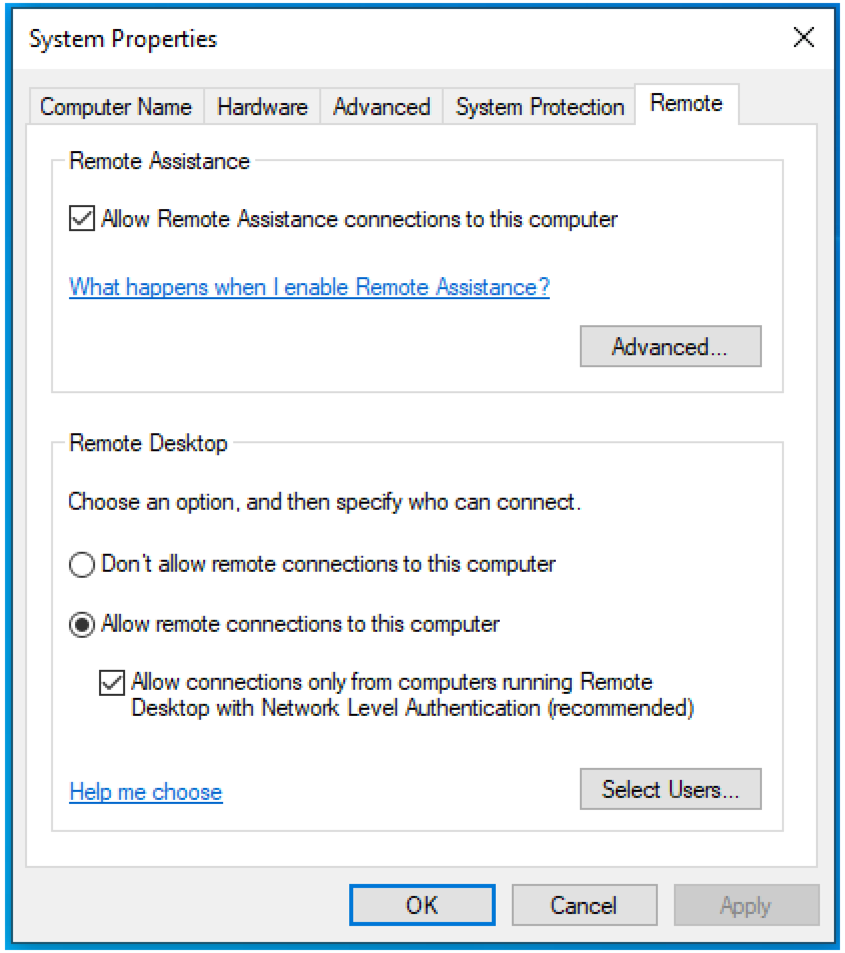


Computer: 192.168.8.102

User name: admin

You will be asked for credentials when you connect.

RDP Server Configuration



Remote Assistance

☑ Allow Remote Assistance connections to this computer

What happens when I enable Remote Assistance?

Remote Desktop

Choose an option, and then specify who can connect.

○ Don't allow remote connections to this computer

● Allow remote connections to this computer

☑ Allow connections only from computers running Remote Desktop with Network Level Authentication (recommended)

Help me choose

Telnet

Old style remote control protocol

Provides client with a command prompt on a remote device

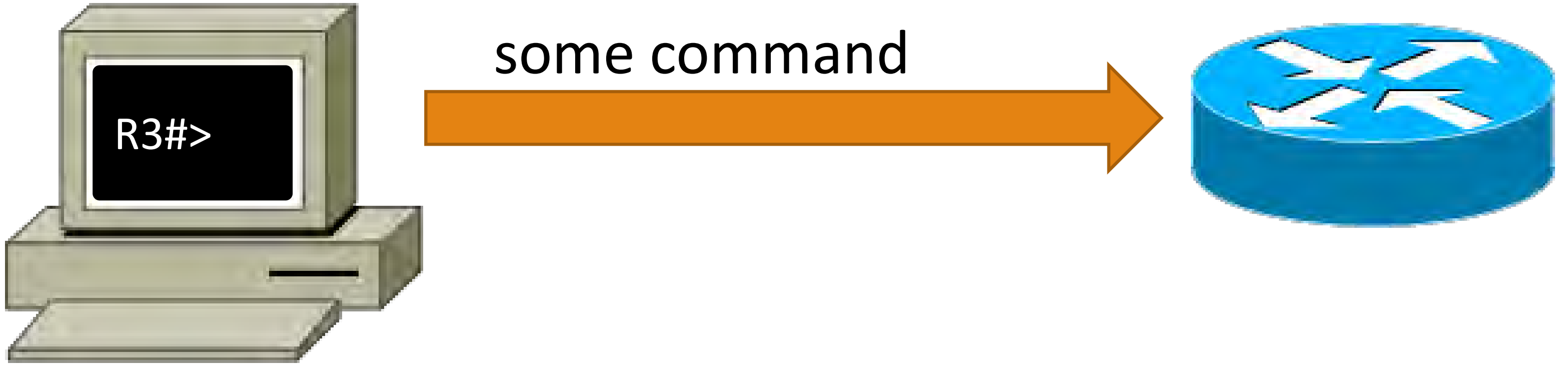
TCP Port 23

All transmissions are sent and received in clear text

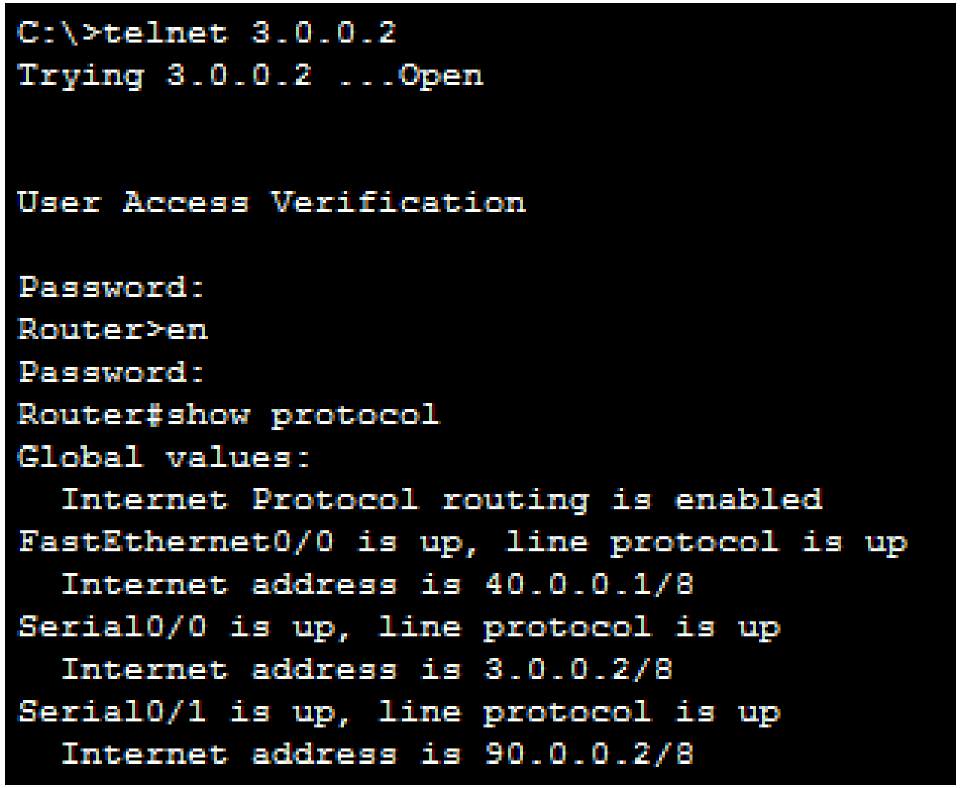
- Telnet client can be used to test open ports (see how / if they respond)

Telnet service automatically installed in Cisco devices (needs to be configured)

Desktop operating systems need to have it installed / enabled



Telnet Example



```
C:\>telnet 3.0.0.2
Trying 3.0.0.2 ...Open


User Access Verification

Password:
Router>en
Password:
Router#show protocol
Global values:
  Internet Protocol routing is enabled
FastEthernet0/0 is up, line protocol is up
  Internet address is 40.0.0.1/8
Serial0/0 is up, line protocol is up
  Internet address is 3.0.0.2/8
Serial0/1 is up, line protocol is up
  Internet address is 90.0.0.2/8
```

Secure Shell (SSH)

Encrypted replacement for Telnet

Microsoft requires a third-party app such as PuTTY (client) and OpenSSH (server)

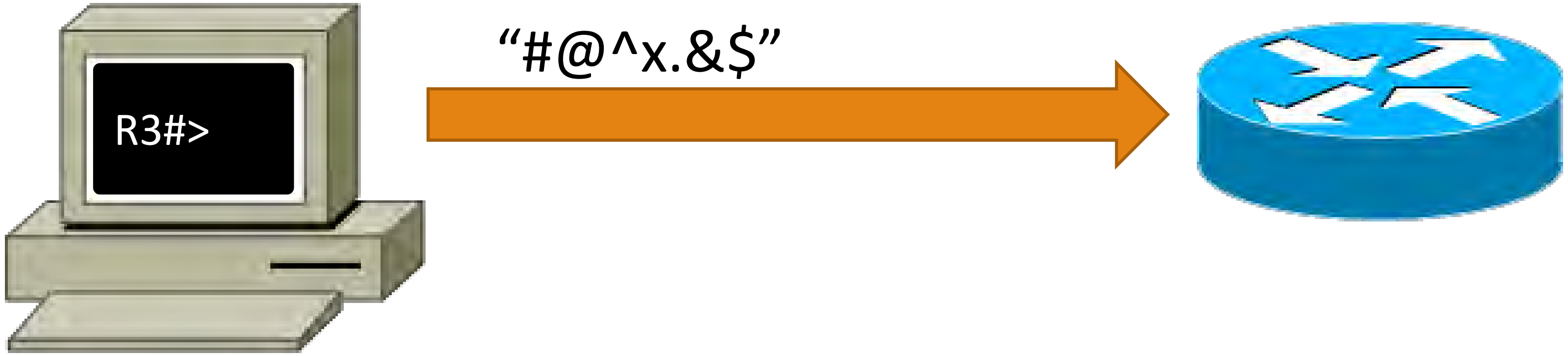
Both sides trade public keys to encrypt the session

- Most SSH applications can create their own public/private key pair

Also includes Secure Copy (SCP) and secure FTP (SFTP)

Also known as Secure Socket Shell

TCP port 22



Virtual Network Computing (VNC)

Open source desktop sharing/remote control system

Server component of VNC runs on the computer that you want to control

Client component of VNC runs on the computer you will use to make the connection

Both client and server can run on Linux, Windows, macOS, Android, iOS (you can mix and match)

Uses TCP 5900 (configurable)

If you use a web client, uses TCP 5800

Session is encrypted

Has a variety of “flavors” such as TightVNC, RealVNC, UltraVNC, etc.

File Sharing Protocols

Server Message Block (SMB)

Microsoft File and Print protocol

Used to access shared folders, drives, and printers

Originally TCP 139 using NetBIOS over TCP/IP

Updated by Microsoft and renamed to Common Internet File System (CIFS) TCP 445

Now referred to as SMB 3.0 TCP 445

Was reverse-engineered for Linux/UNIX

- Server service is called “Samba”

Subject to many exploits including:

- EternalBlue
- WannaCry ransomware

File Transfer Protocol

TCP 21 = command port

TCP 20 = data port

Requires user to authenticate

- Can be configured to accept “anonymous” as the username, with any password

All transmissions are in clear text

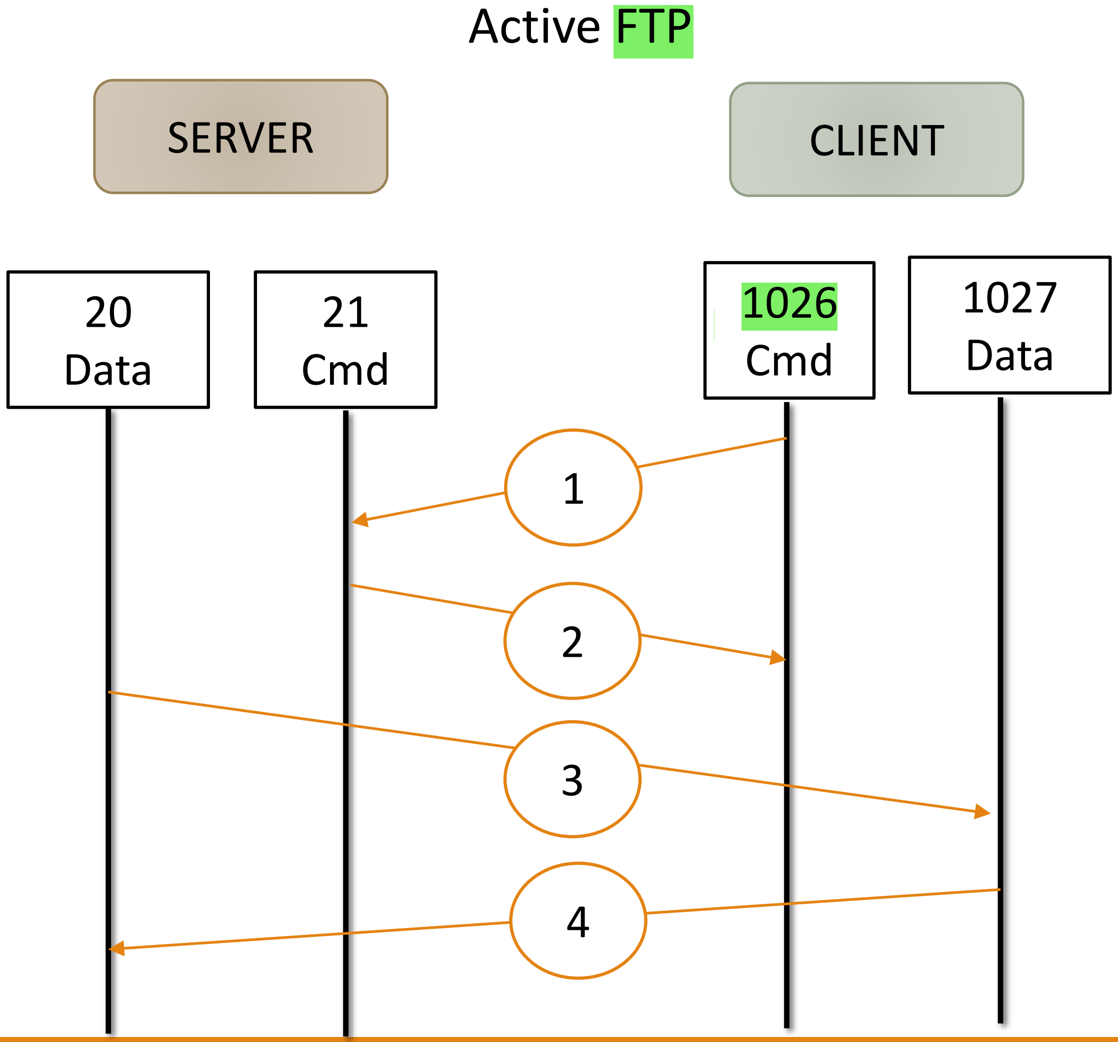
Active Mode:

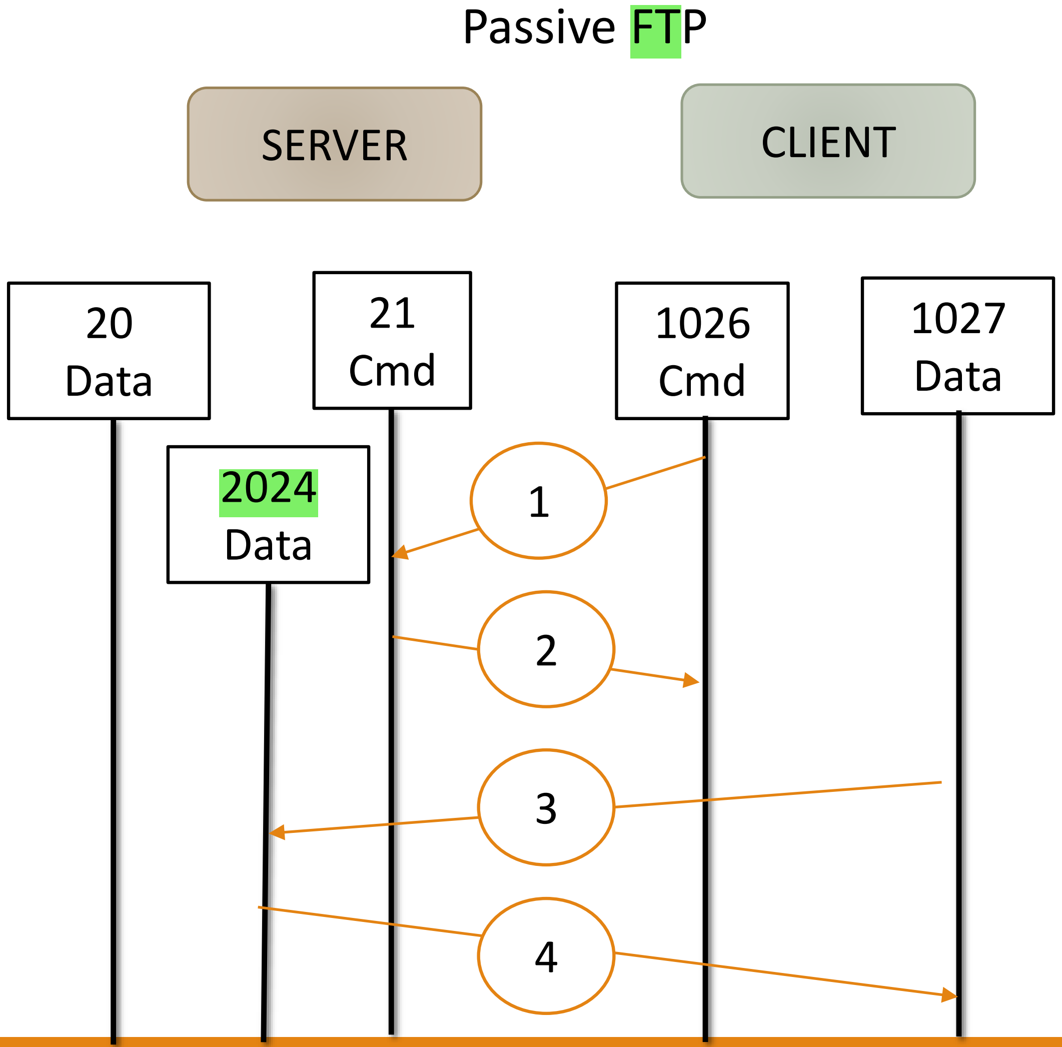
- Client tells the server what port it’s using
- The server starts the data connection in a separate session
- The client’s firewall may interpret that connection attempt as an unauthorized outside connection and block the server’s data connection
- The administrator must open ports likely to be used by the data connection

Passive Mode:

- The client starts the data connection in a separate session
- The client’s firewall notes the client’s outbound connection, and permits the server’s inbound response

FTP Handshake





Secure File Transfer Protocol (SFTP)

Secure File Transfer Protocol is also called SSH File Transfer Protocol

Encrypts the file transfer

Is a network protocol for accessing, transferring and managing files on remote systems

Requires that the client be authenticated by the server

Allows businesses to securely transfer billing data, funds and data recovery files

Runs on TCP port 22 as part of the SSH suite

You can change the port if desired

Trivial File Transfer Protocol (TFTP)

UDP port 69

Simplified version of FTP

No authentication

All transmissions are in clear text

Often used to save/load router and switch operating systems, updates, and configuration files

Because it uses UDP with no flow control or error checking, it is not well suited to cross multiple routers or traverse many network segments

Network File Share (NFS)

File sharing protocol for Unix / Linux

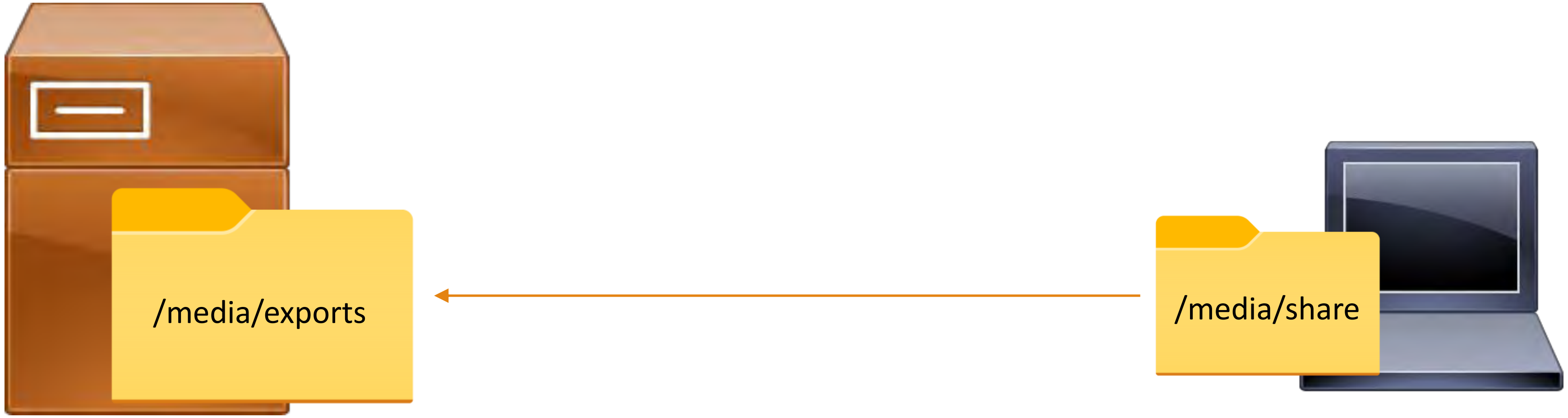
Uses TCP 2049

NFS v3 also uses the portmapper service at TCP or UDP 111

- Consulted to get the port number for NFS and other services

NFS v4 does not require the portmapper service

NFS Example



```
$ sudo mkdir -p /media/exports
```

```
$ sudo mount –t nfs4
192.168.1.10:/media/exports /media/share
```

Web Protocols

Hyper Text Transfer Protocol (HTTP)

Used to carry web traffic

TCP 80

Stateless

- Doesn’t attempt to remember any previous transactions or commands in the session
- The server or client can send keepalive packets for a short while to keep the session active

Transmissions are in clear text

- It’s not secure for transactions

post is a smal amnput of data

uploadign a larghe ampount of data

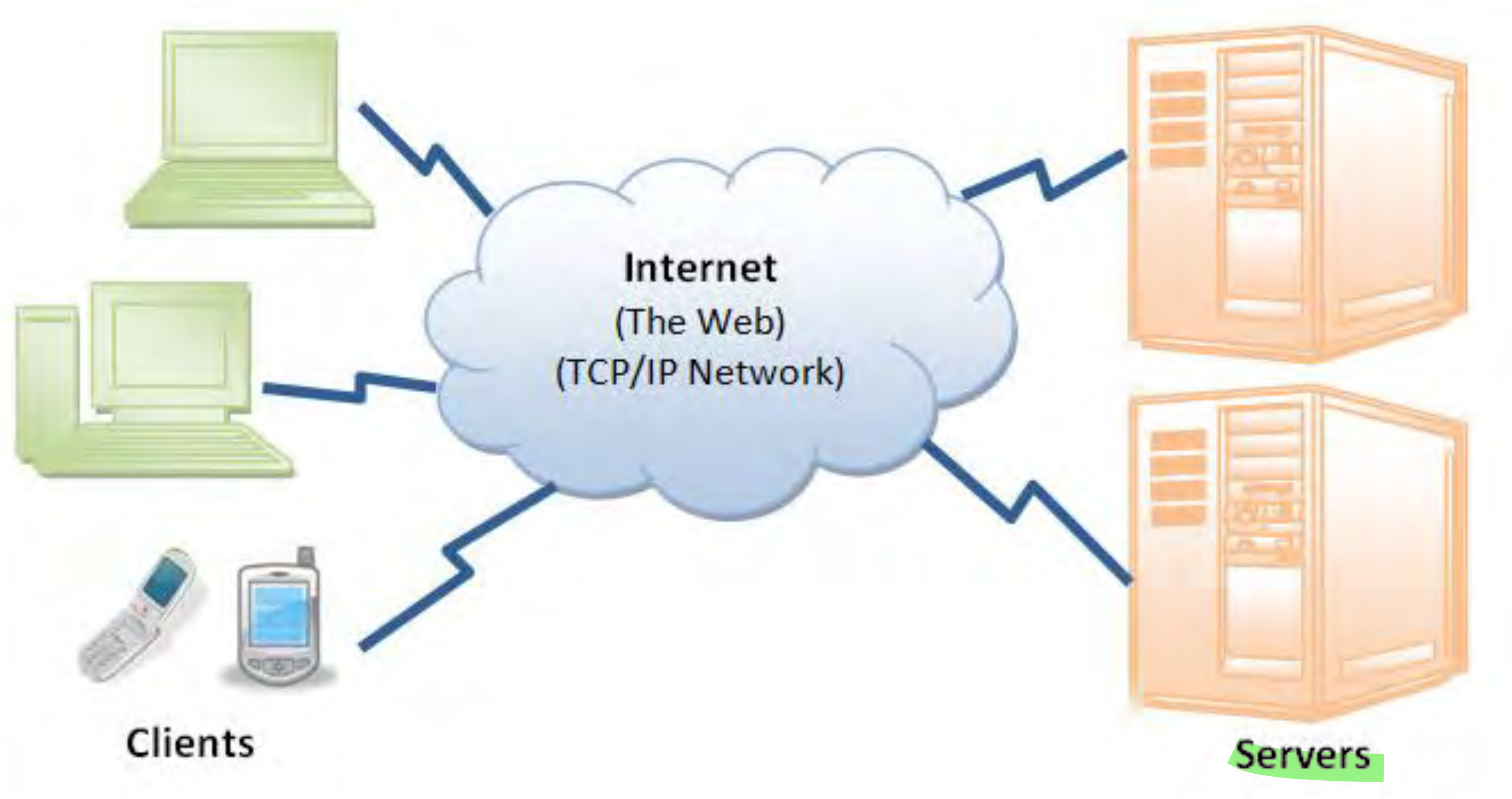
Has the following requests (methods): GET, POST, PUT, HEAD, DELETE, CONNECT, TRACE, OPTIONS

thi s can be uused toi attack another website through coneecting to the first one

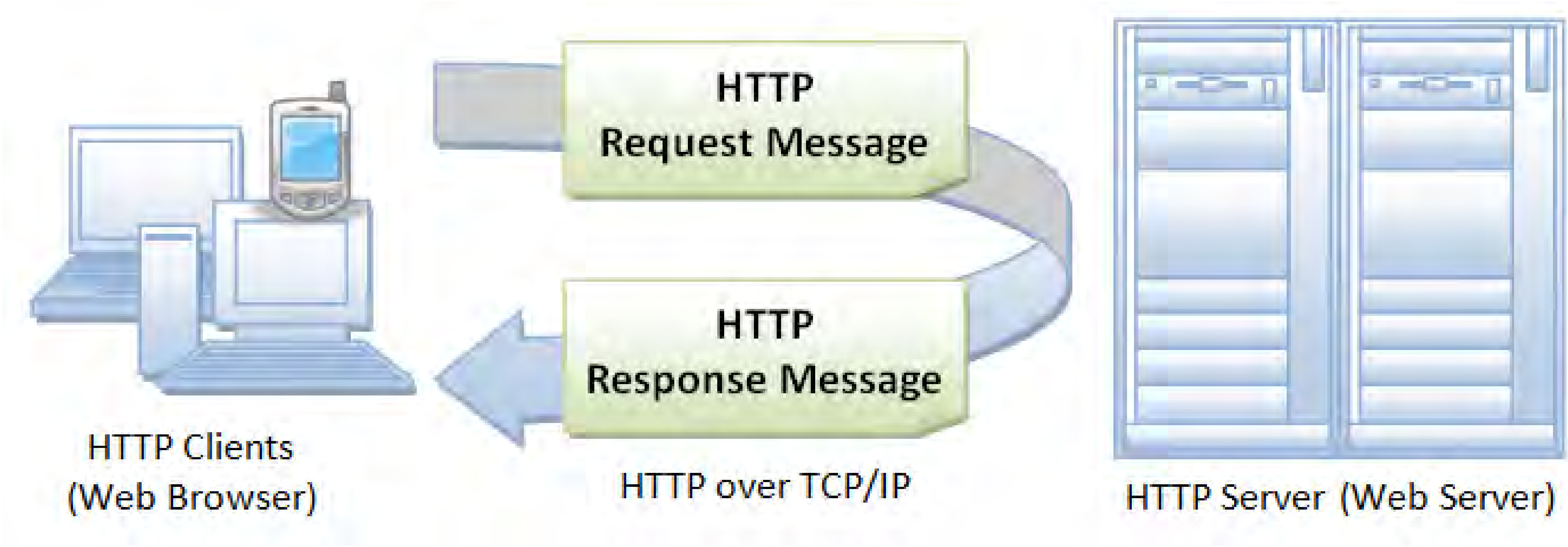
Can be used like FTP to upload and download files

- FTP has better performance than HTTP for bulk file transfer

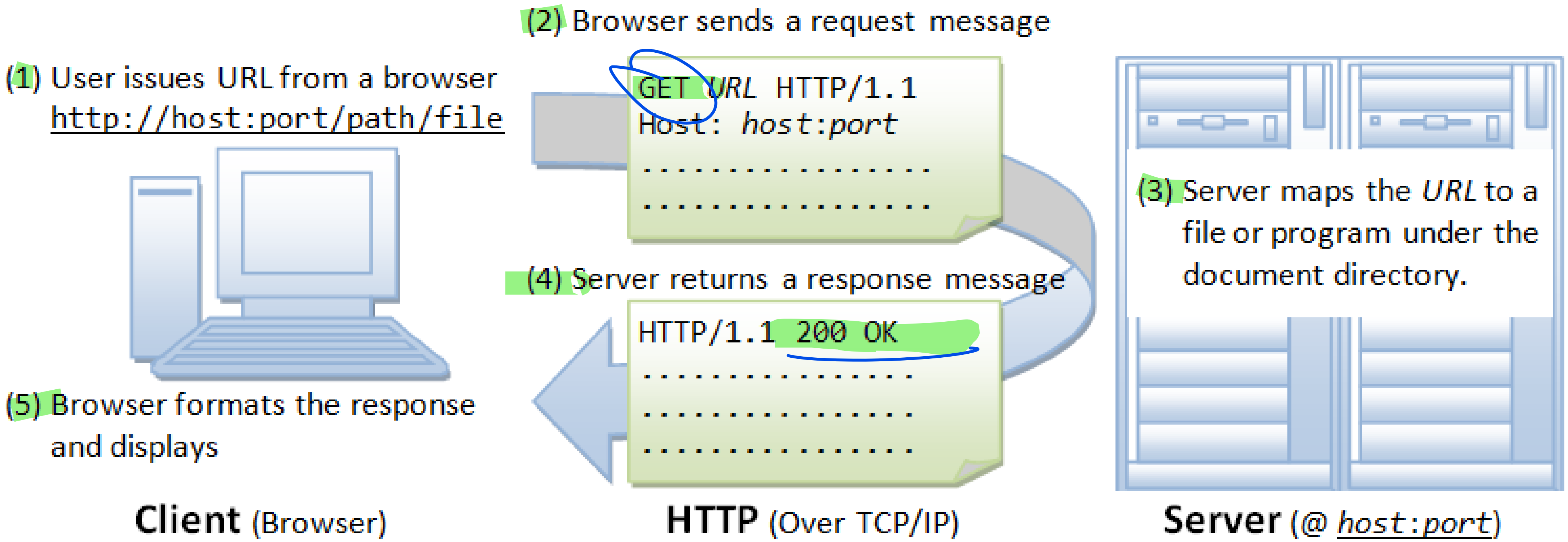
Web Servers



HTTP Process



HTTP GET Request



(1) User issues URL from a browser
http://host:port/path/file

(2) Browser sends a request message

```
GET URL HTTP/1.1
Host: host:port
..................
..................
```

(3) Server maps the *URL* to a file or program under the document directory.

(4) Server returns a response message

```
HTTP/1.1 200 OK
................
................
................
```

(5) Browser formats the response and displays

Client (Browser)

HTTP (Over TCP/IP)

Server (@ *host:port*)

Uniform Resource Locator (URL)

Used to uniquely identify a resource over the web

Has the following syntax:

protocol://hostname:port/path-and-file-name

http://www.company123.com/docs/index.html

http://extranet.company123.com:8888/login.aspx

Protocol: The application-level protocol used by the client and server

- HTTP, HTTPS, FTP, etc.

Hostname: The DNS domain name

- www.company123.com
- IP address (e.g., 192.128.1.2) of the server

Port: The TCP port number that the server is listening for incoming requests from the clients (typically 80 or 443)

Path-and-file-name: The name and location of the requested resource, under the server document base directory

Note: Some browsers can use additional protocols/commands such as ftp:// file:// mms:// etc.

Hyper Text Transfer Protocol Secure (HTTPS)

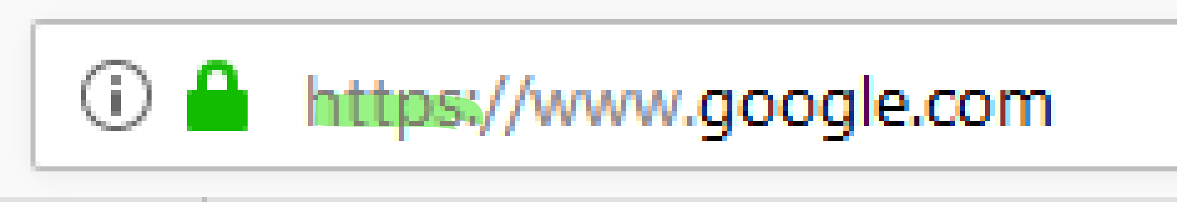
HTTP over SSL or TLS

TCP 443

Stateless (like HTTP)

Should not be confused with SSL or TLS (Layer 6 protocols)

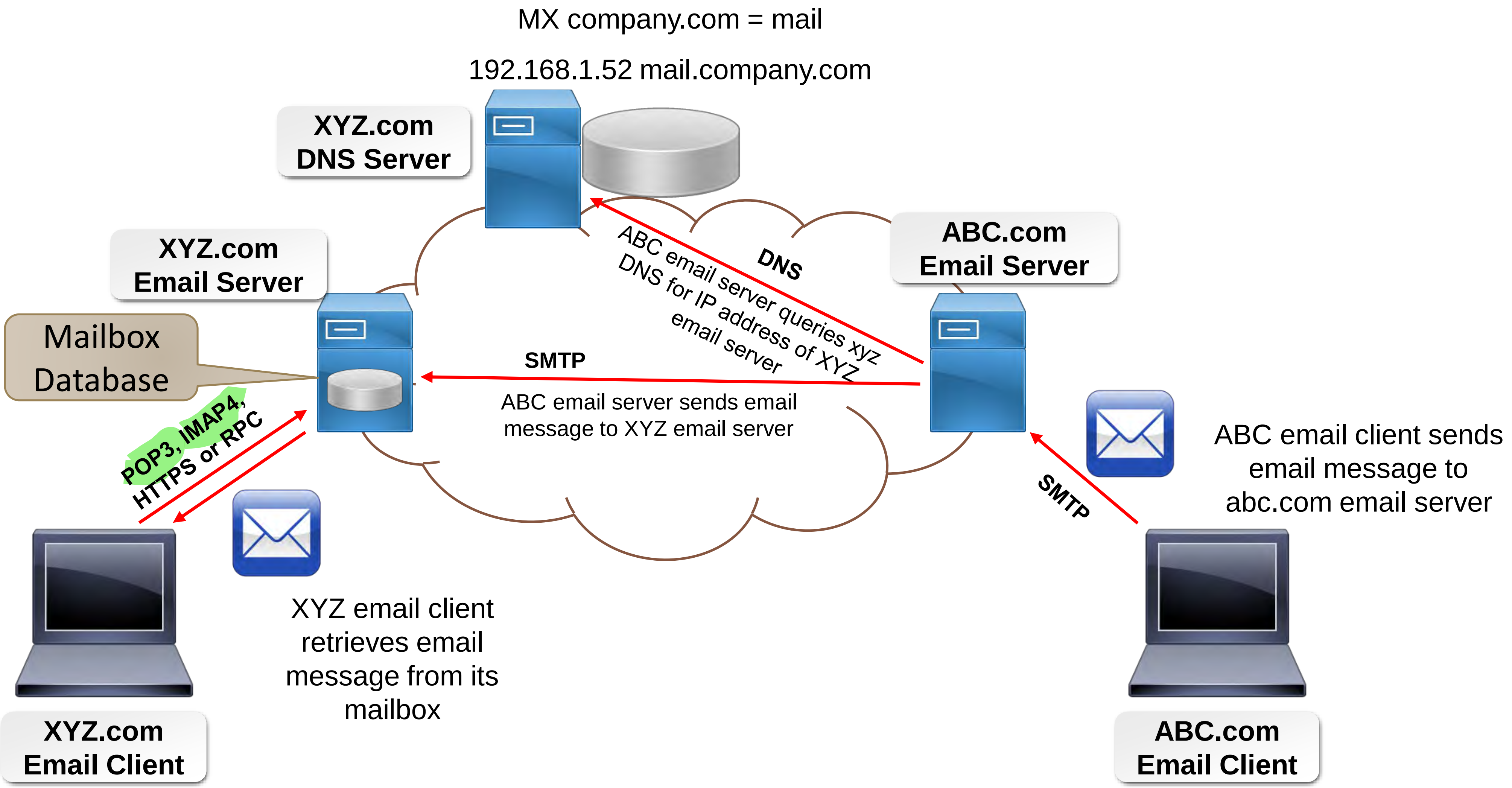
- HTTPS uses Transport Layer Security (TLS) to encrypt data
- TLS latest version is 1.3
- Older versions used Secure Sockets Layer (SSL)
- SSL latest version is 3.0



https://www.google.com

Email Protocols

Email Process



MX company.com = mail

192.168.1.52 mail.company.com

XYZ.com DNS Server

XYZ.com Email Server

Mailbox Database

ABC.com Email Server

DNS

ABC email server queries xyz DNS for IP address of XYZ email server

SMTP

ABC email server sends email message to XYZ email server

POP3, IMAP4, HTTPS or RPC

SMTP

ABC email client sends email message to abc.com email server

XYZ email client retrieves email message from its mailbox

XYZ.com Email Client

ABC.com Email Client

Simple Mail Transfer Protocol (SMTP)

Internet (TCP/IP) standard for electronic mail (email) transmission

Transmissions are in clear text

Used for sending email

- Client to server
- Server to server

TCP port 25 (IANA also allocated UDP 25 but it’s not used today)

Has encrypted versions (SMTP using SSL/TLS):

- TCP port 587
- TCP port 465 (legacy)

Post Office Protocol (POP3)

One of the most commonly used Internet mail protocols for retrieving emails from a server by a local client

Supported by all modern email clients and email servers

Allows you to download email messages on your local computer and read them even when you are offline

- Messages are downloaded locally and removed from the email server

POP3 protocol works on two ports:

- Port 110 is the default POP3 clear text non-encrypted port
- Port 995 uses SSL/TLS encrypted secure port

Internet Message Access Protocol (IMAP4)

A mail protocol used for accessing email on a remote web server from a local client

IMAP is one of the most commonly used Internet mail protocols for retrieving emails

Supported by all modern email clients and web servers

- Messages stay on Email server
- Allows interactive session with Email server

IMAP allows simultaneous access by multiple clients

Suitable if a user is going to access email from different locations or by multiple users

TCP 143 (clear text)

IMAP4/SSL uses TCP 993

HTTP / HTTPS for Email

You can also use a browser to retrieve your email

- This requires that the email server also have a webserver front end

The browser uses frames and scripting to organize your inbox into a collection of panes

The main content pane shows a list of emails

When you click an email, it takes up the main pane

Database Protocols

Structured Query Language (SQL)

The language used to communicate with a relational database

Most SQL servers can be configured to accept remote client connections

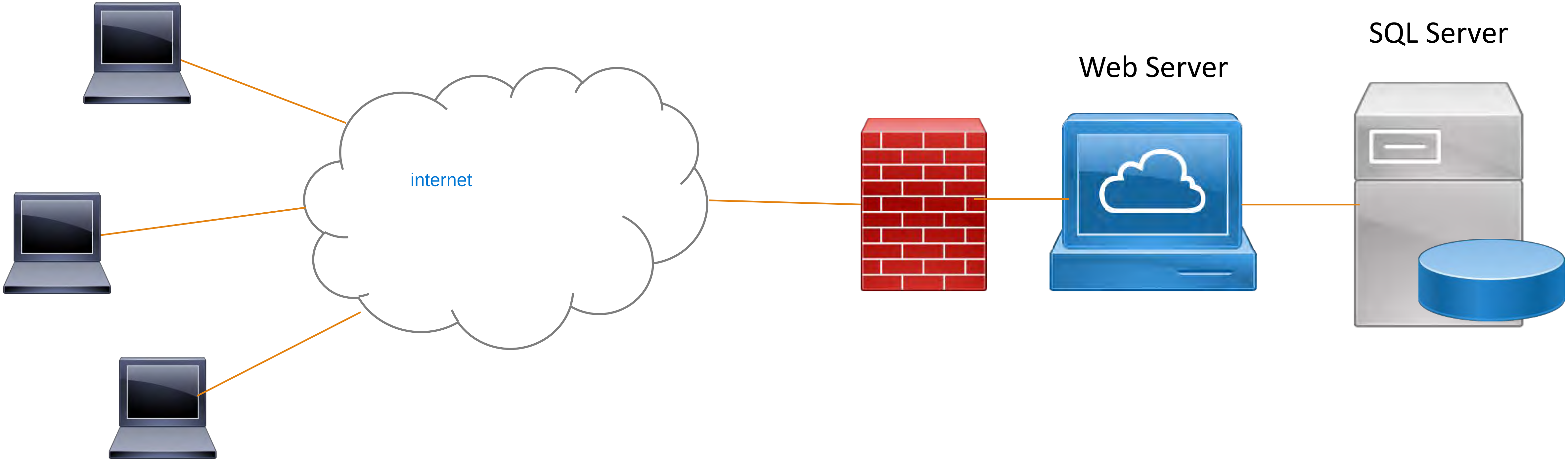
SQL servers often provide the database "back end" for a web server

Examples:

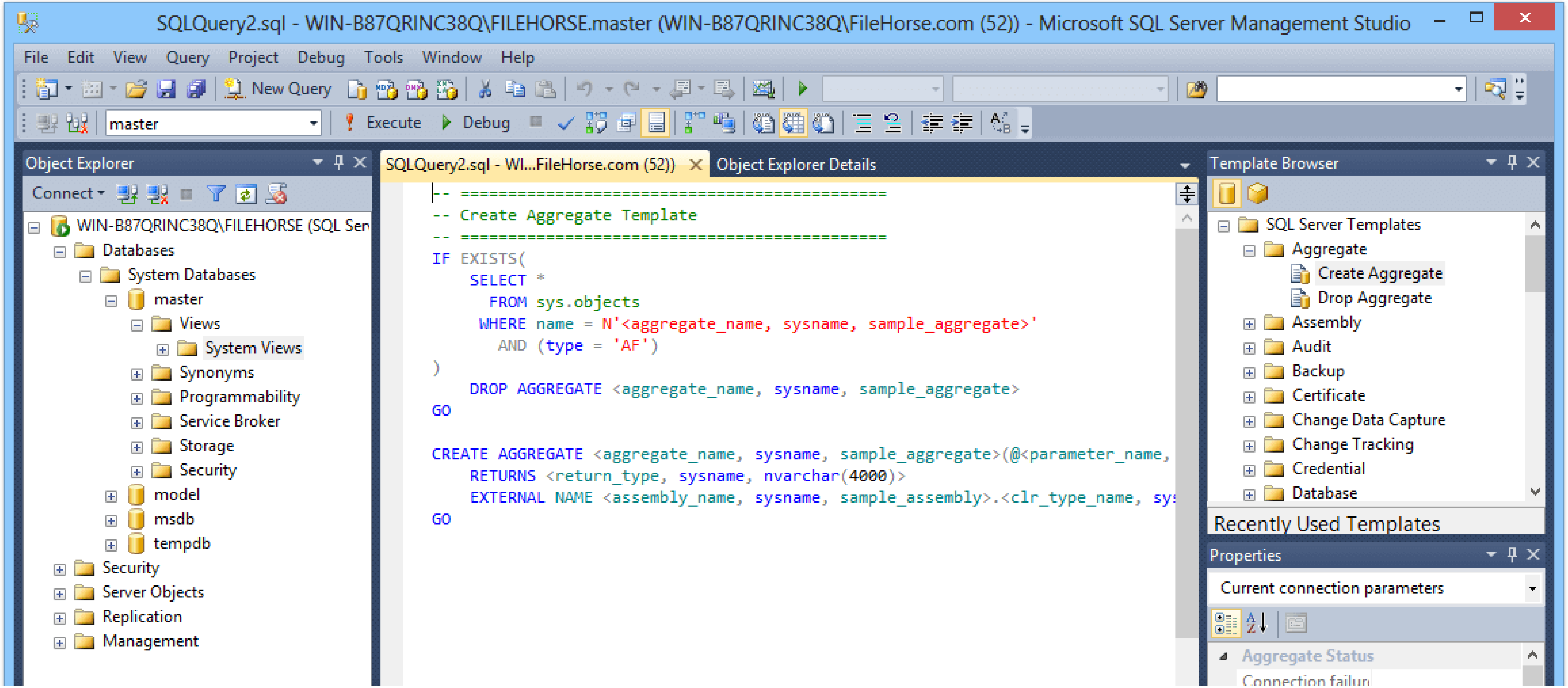
- MSSQL (Microsoft) TCP 1433
- SQLnet (Oracle) TCP 1521
- MySQL (Open source) TCP 3306
- SQLite (Open source – mobile apps)

important

Web Server with SQL Server Back End Example



MSSQL Management Studio Example

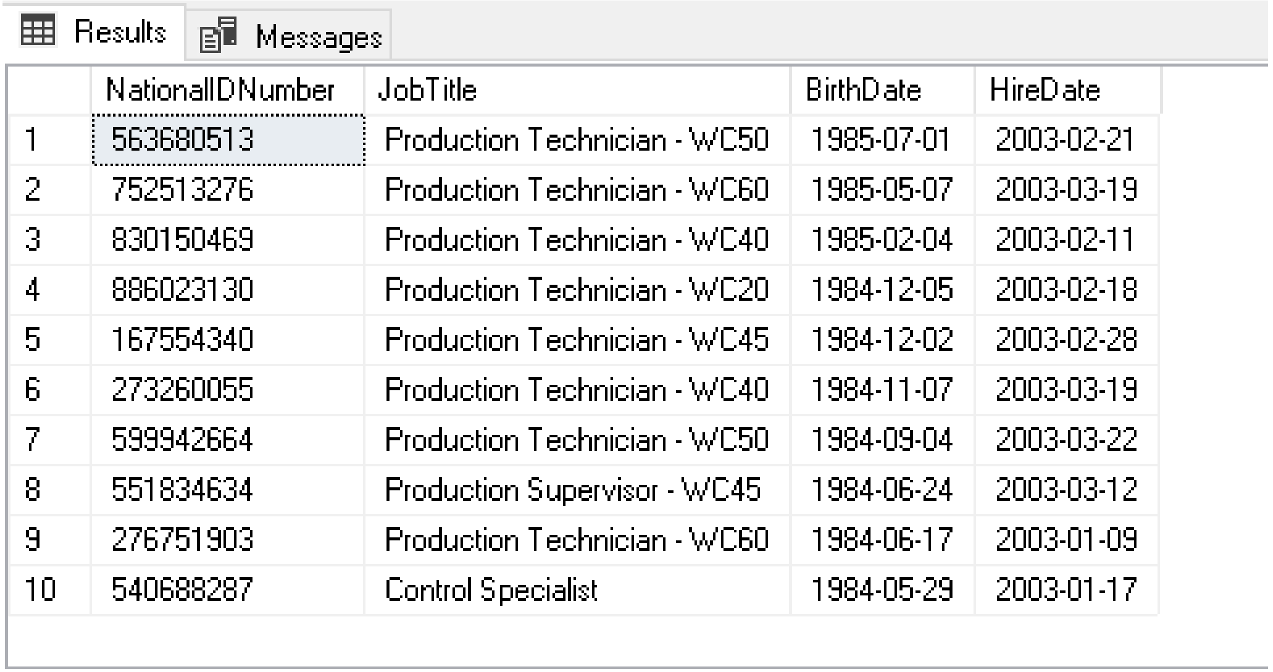


```
-- =============================================
-- Create Aggregate Template
-- =============================================
IF EXISTS(
    SELECT *
      FROM sys.objects
     WHERE name = N'<aggregate_name, sysname, sample_aggregate>'
       AND (type = 'AF')
)
    DROP AGGREGATE <aggregate_name, sysname, sample_aggregate>
GO

CREATE AGGREGATE <aggregate_name, sysname, sample_aggregate>(@<parameter_name,
    RETURNS <return_type, sysname, nvarchar(4000)>
    EXTERNAL NAME <assembly_name, sysname, sample_assembly>.<clr_type_name, sys
GO
```

SQL Example

```
SELECT TOP (10) NationalIDNumber,
                JobTitle,
                BirthDate,
                HireDate
FROM HumanResources.Employee
ORDER BY BirthDate DESC;
GO
```



	NationalIDNumber	JobTitle	BirthDate	HireDate
1	563680513	Production Technician - WC50	1985-07-01	2003-02-21
2	752513276	Production Technician - WC60	1985-05-07	2003-03-19
3	830150469	Production Technician - WC40	1985-02-04	2003-02-11
4	886023130	Production Technician - WC20	1984-12-05	2003-02-18
5	167554340	Production Technician - WC45	1984-12-02	2003-02-28
6	273260055	Production Technician - WC40	1984-11-07	2003-03-19
7	599942664	Production Technician - WC50	1984-09-04	2003-03-22
8	551834634	Production Supervisor - WC45	1984-06-24	2003-03-12
9	276751903	Production Technician - WC60	1984-06-17	2003-01-09
10	540688287	Control Specialist	1984-05-29	2003-01-17

Voice Protocols

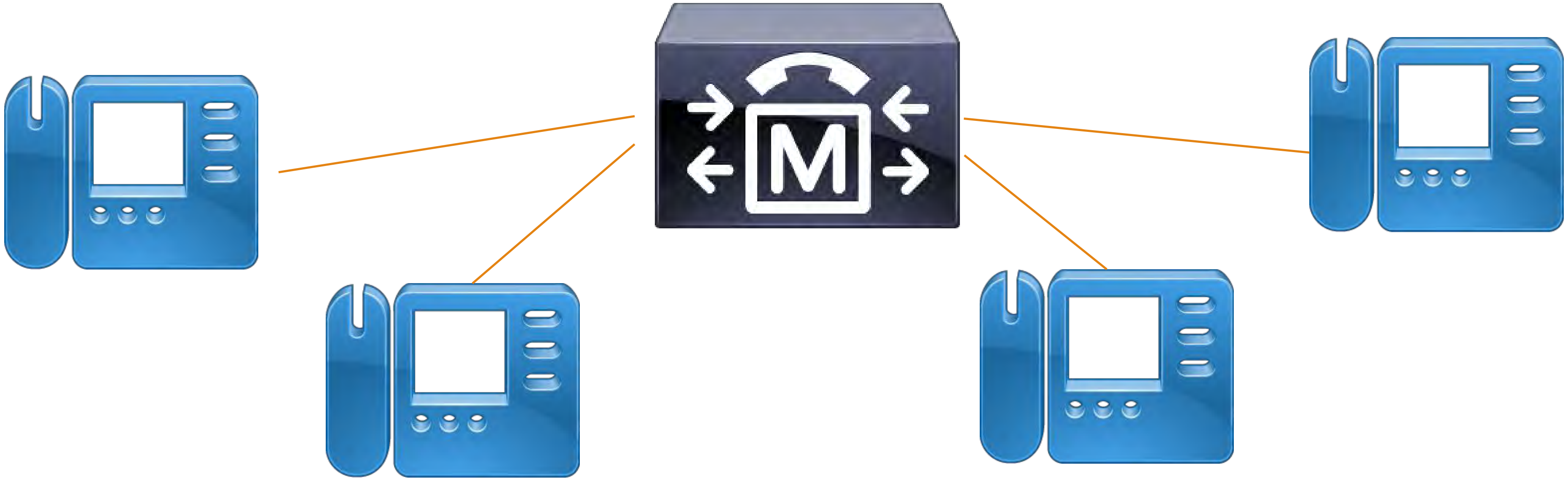
Session Initiation Protocol (SIP)

Establishes, manages, tears down Voice-over-IP (VoIP) calls and multimedia conferences

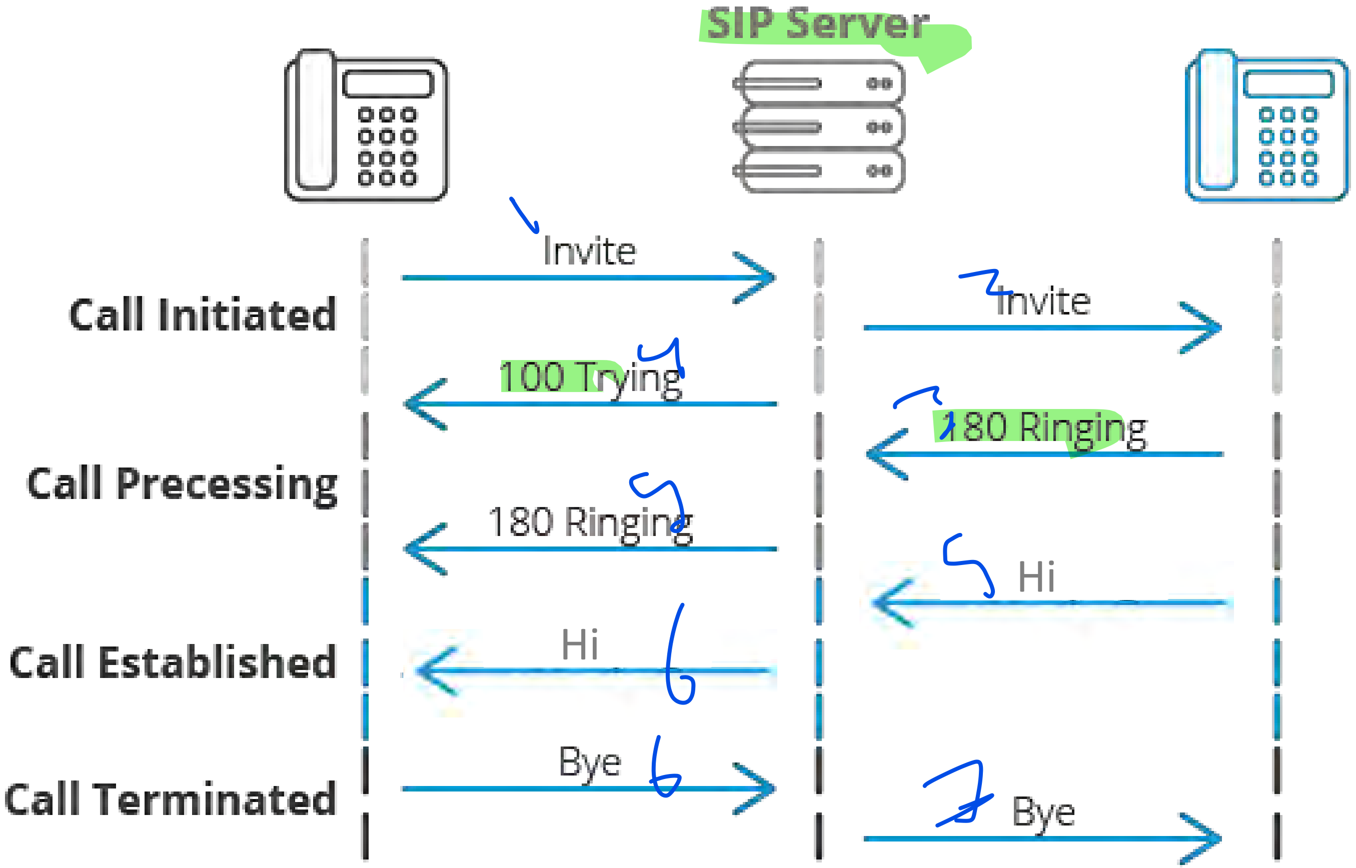
The SIP protocol is a member of the VoIP Protocol Family

Internet Engineering Task Force (IETF) standard

TCP and UDP 5060 (unencrypted) and 5061 (TLS encrypted)



SIP Process


SIP Server
Call Initiated
Call Precessing
Call Established
Call Terminated
1
Invite
2
Invite
4
100 Trying
3
180 Ringing
5
180 Ringing
5
Hi
6
Hi
6
Bye
7
Bye

Real-time Transport Protocol (RTP)

Carries audio and video over IP

Works with SIP or H.323 for VoIP calls and multimedia video conferences

Payload will have various compression (codec) formats such as G.711 or MPEG-4

UDP with whatever available port (1024 – 65535)

Secure RTP (SRTP) is the encrypted version

H.323

International Telecommunications Union (ITU) standard

Defines the protocols to provide audio-visual communication sessions on any packet-switched network

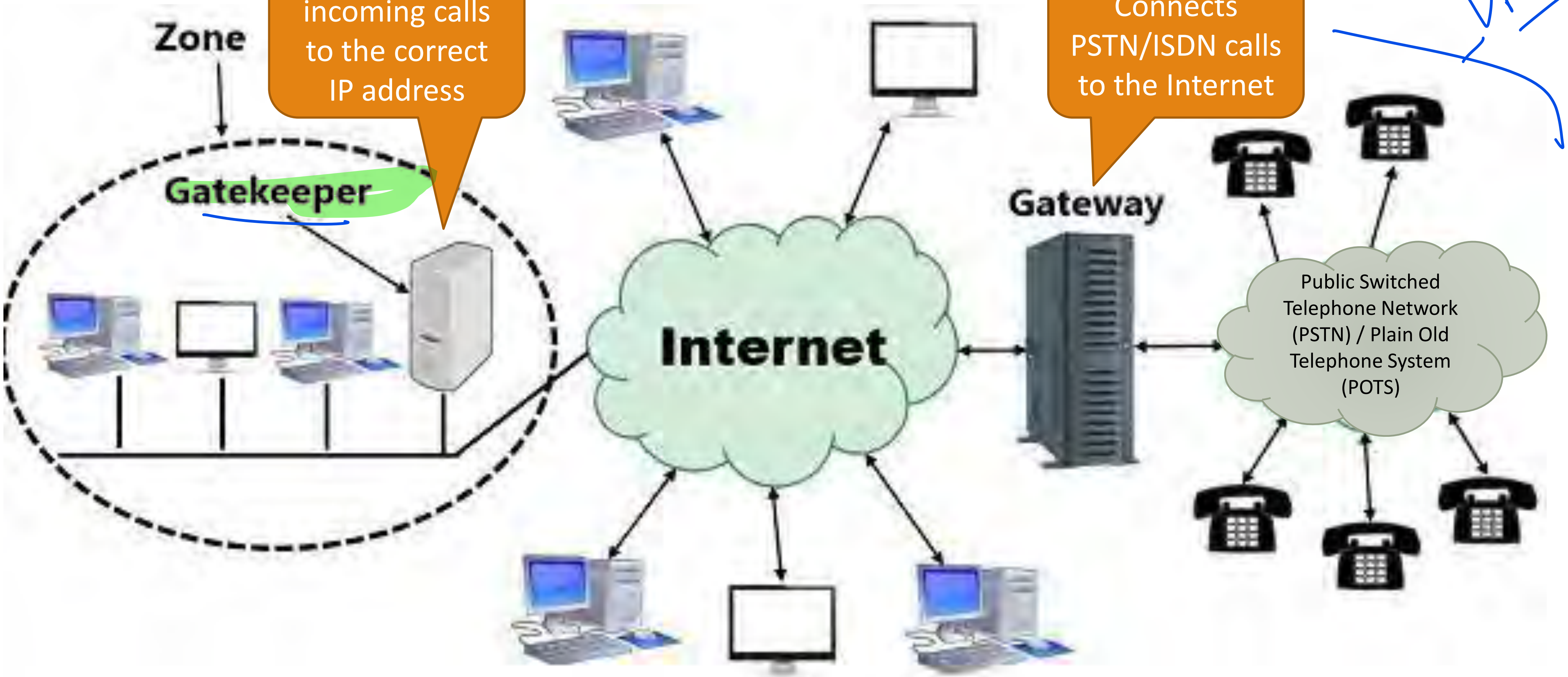
TCP port 1720 used during call setup negotiation

Pre-dates SIP

Still used by Cisco WebEx and Microsoft Skype for Business, as well as others

H.323 Architecture

H.323



Zone
Gatekeeper
Internet
Gateway
Public Switched Telephone Network (PSTN) / Plain Old Telephone System (POTS)

IP PBX - Routes incoming calls to the correct IP address

Connects PSTN/ISDN calls to the Internet

Security Protocols

IP Security (IPSEC)

Most popular VPN mechanism today

Two protocols at Layer 3 that digitally sign and optionally encrypt an IP packet

Can be used between:

- Host and host
- Router and router
- Host and firewall / router / VPN server

Note: “VPN” in this topic refers to a traditional IPSEC VPN as opposed to anonymous browsing using HTTPS and a chain of proxy servers

IPSEC Protocols

Authentication Header (AH)

- Protocol ID 51
- Used to digitally sign IP header of packet
- MD5, SHA

Encapsulating Security Payload (ESP)

- Protocol ID 50
- Used to encrypt and digitally sign the data payload
- DES, 3DES, AES

Internet Key Exchange (IKE) v2

- UDP 500
- Used to establish the connection
- Phase 1—Negotiate how to authenticate and secure the channel
- Phase 2—Negotiate security associations (SAs) to protect the data

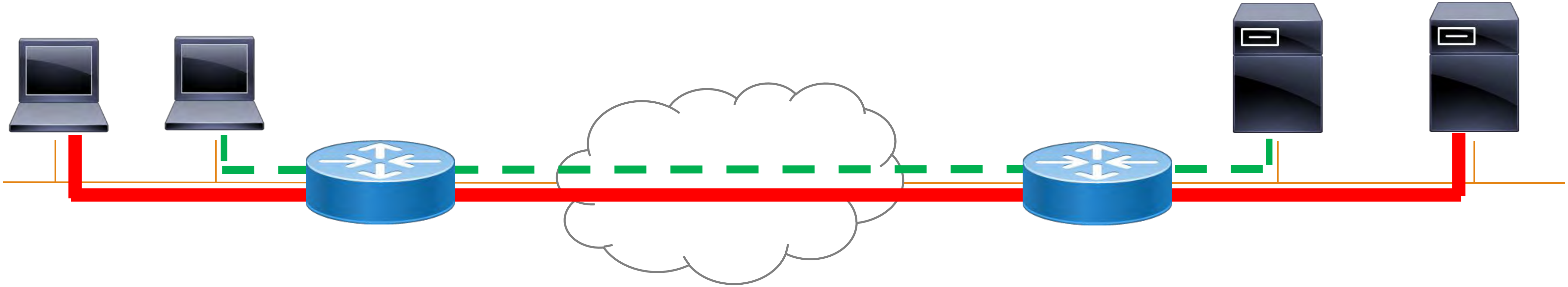
IPSEC Transport Mode

End-to-End

Hosts create the VPN between them

Routers treat it like normal traffic

Other hosts cannot decrypt the traffic



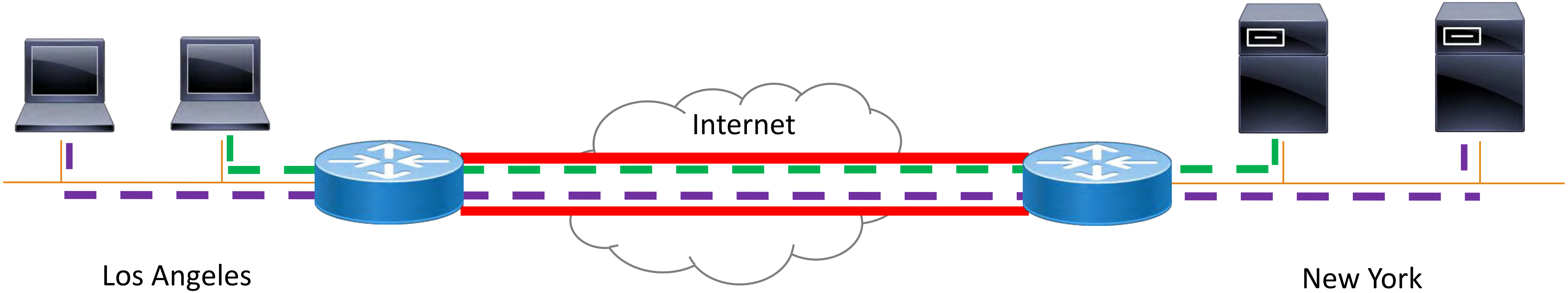
IPSEC Tunnel Mode

Router-to-Router

- Aka “site-to-site VPN”

Hosts are unaware that their data is passing through a secure tunnel

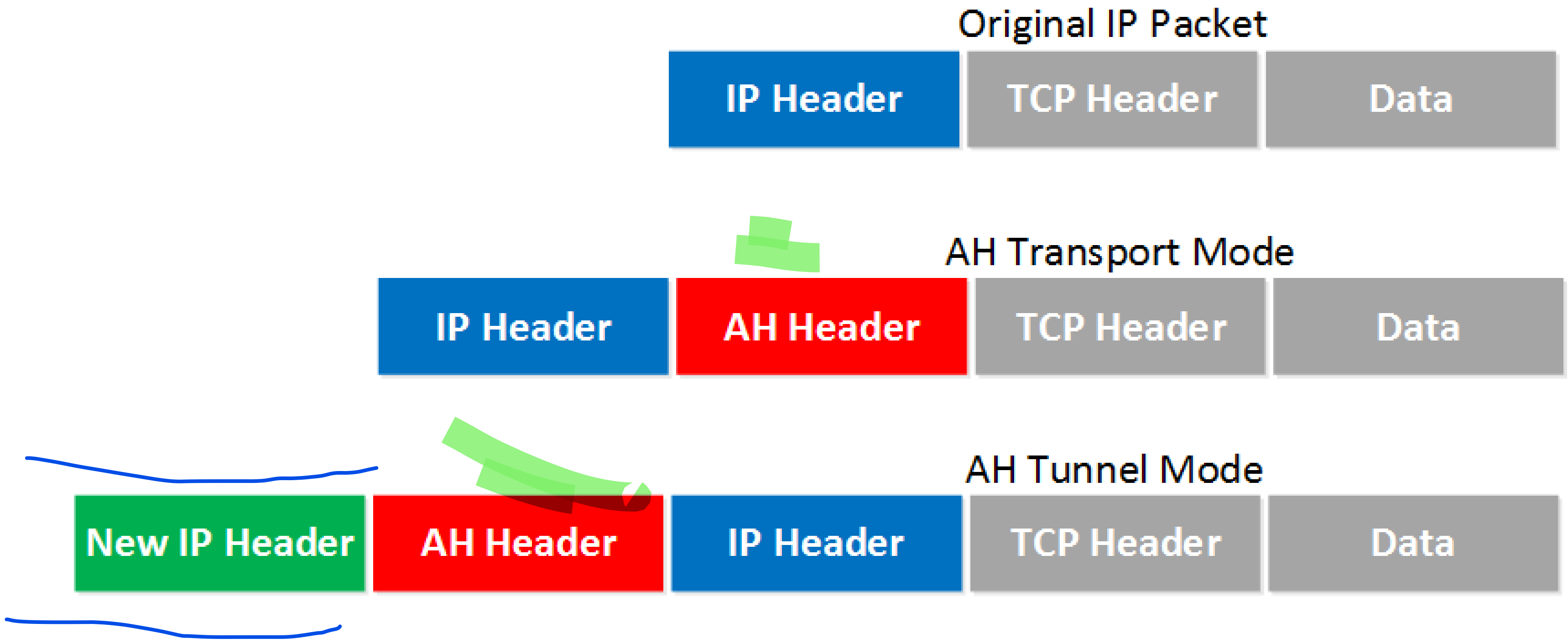
Commonly used to secure traffic between sites



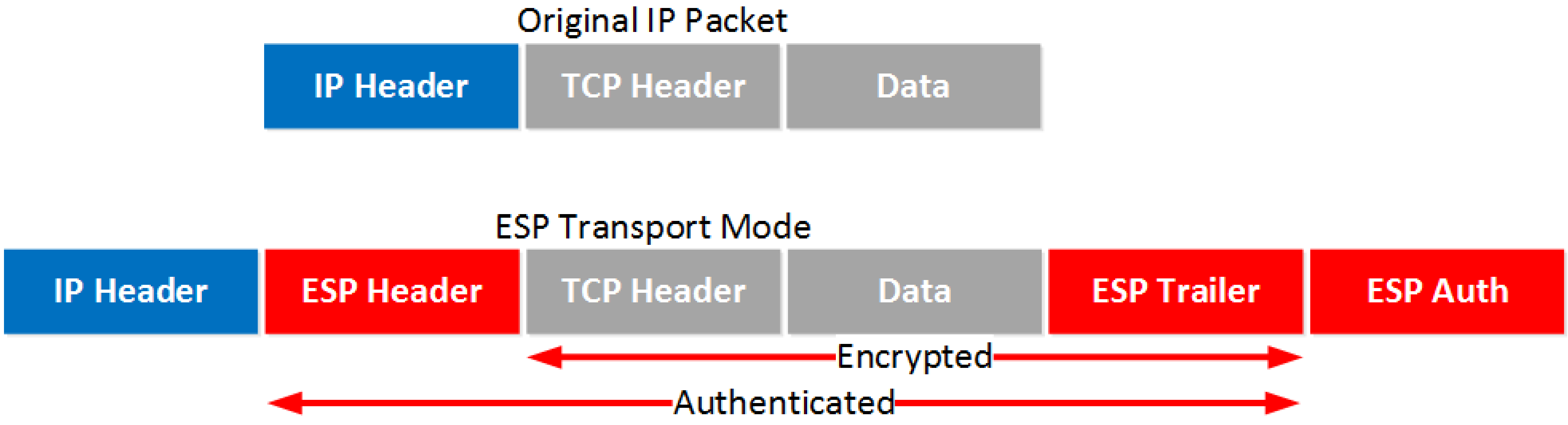
Los Angeles

New York

IPSEC AH Encapsulation



IPSEC ESP Encapsulation



Management Protocols

Syslog

A standard protocol used to send system log or event messages to a specific server, called a syslog server UDP 514

Allows for separation of:

- Message generation
- Message storage
- Message analysis

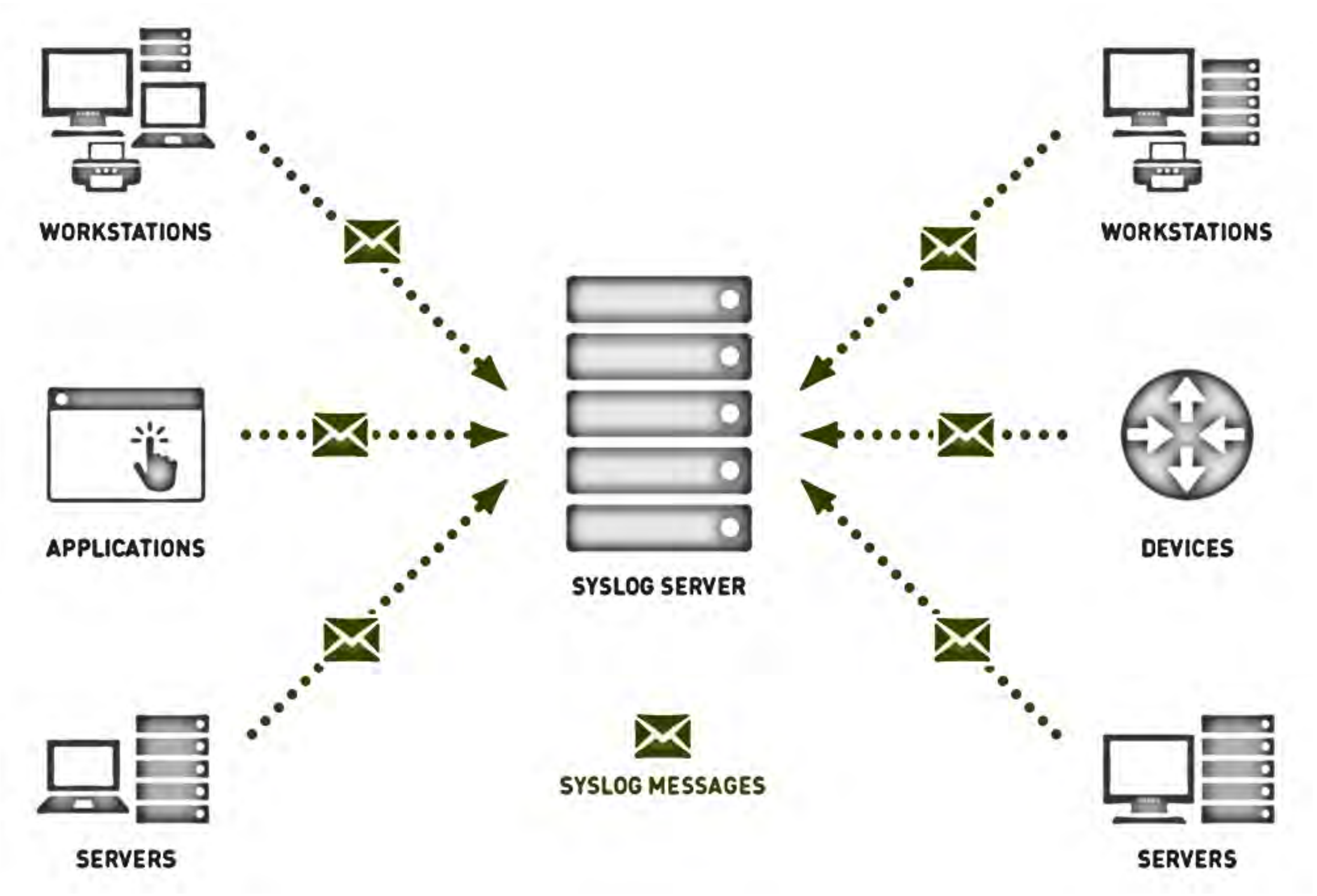
Used to collect various device logs from several different machines in a central location for monitoring and review

- Device and application monitoring
- Management
- Security auditing

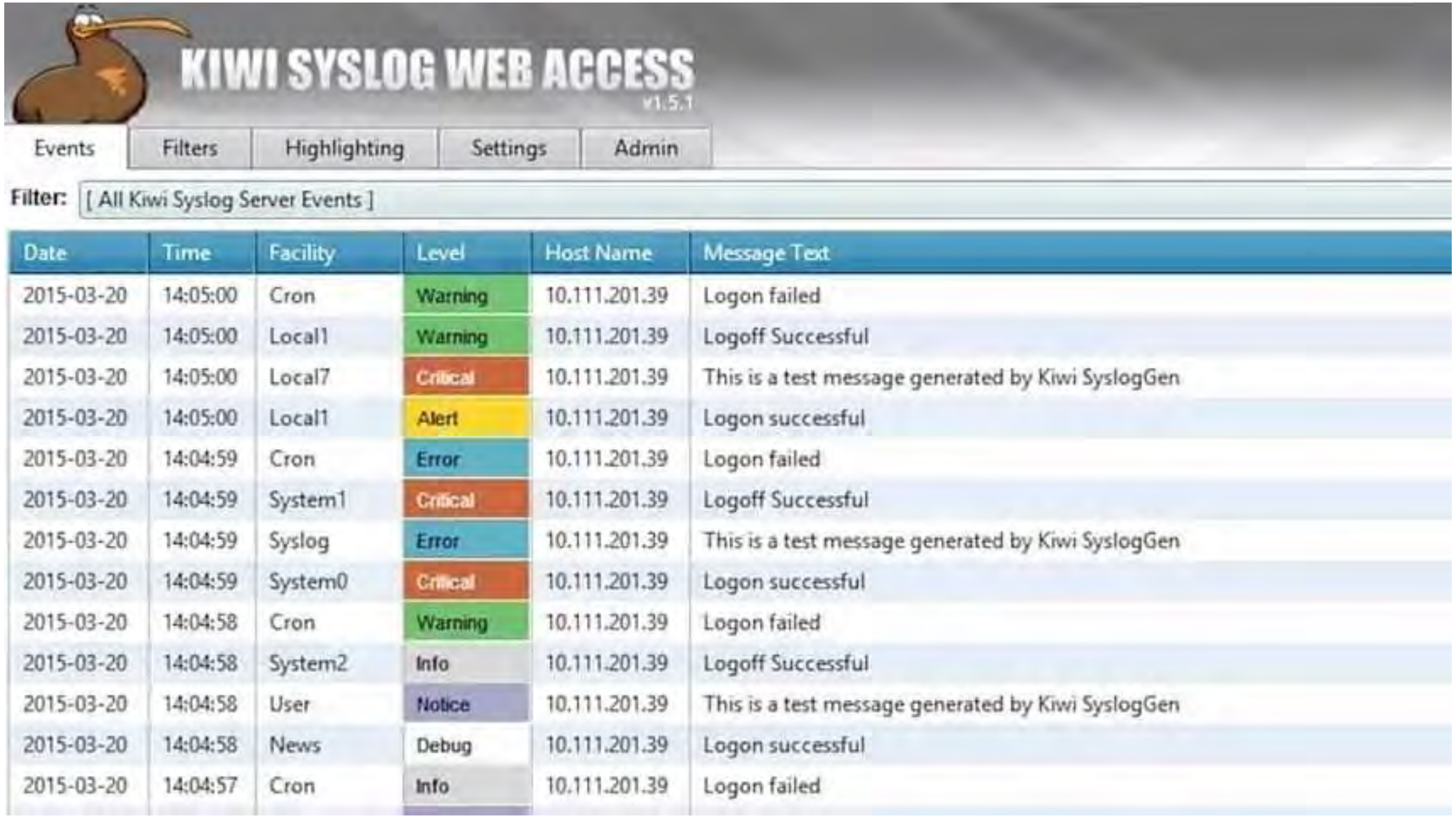
Collects device logs

- Is dependent on the device logging its own events

Syslog Example



Syslog Console Example



Filter: [All Kiwi Syslog Server Events]

Date	Time	Facility	Level	Host Name	Message Text
2015-03-20	14:05:00	Cron	Warning	10.111.201.39	Logon failed
2015-03-20	14:05:00	Local1	Warning	10.111.201.39	Logoff Successful
2015-03-20	14:05:00	Local7	Critical	10.111.201.39	This is a test message generated by Kiwi SyslogGen
2015-03-20	14:05:00	Local1	Alert	10.111.201.39	Logon successful
2015-03-20	14:04:59	Cron	Error	10.111.201.39	Logon failed
2015-03-20	14:04:59	System1	Critical	10.111.201.39	Logoff Successful
2015-03-20	14:04:59	Syslog	Error	10.111.201.39	This is a test message generated by Kiwi SyslogGen
2015-03-20	14:04:59	System0	Critical	10.111.201.39	Logon successful
2015-03-20	14:04:58	Cron	Warning	10.111.201.39	Logon failed
2015-03-20	14:04:58	System2	Info	10.111.201.39	Logoff Successful
2015-03-20	14:04:58	User	Notice	10.111.201.39	This is a test message generated by Kiwi SyslogGen
2015-03-20	14:04:58	News	Debug	10.111.201.39	Logon successful
2015-03-20	14:04:57	Cron	Info	10.111.201.39	Logon failed

Windows Event Log Subscriptions

Windows built-in “syslog” capability

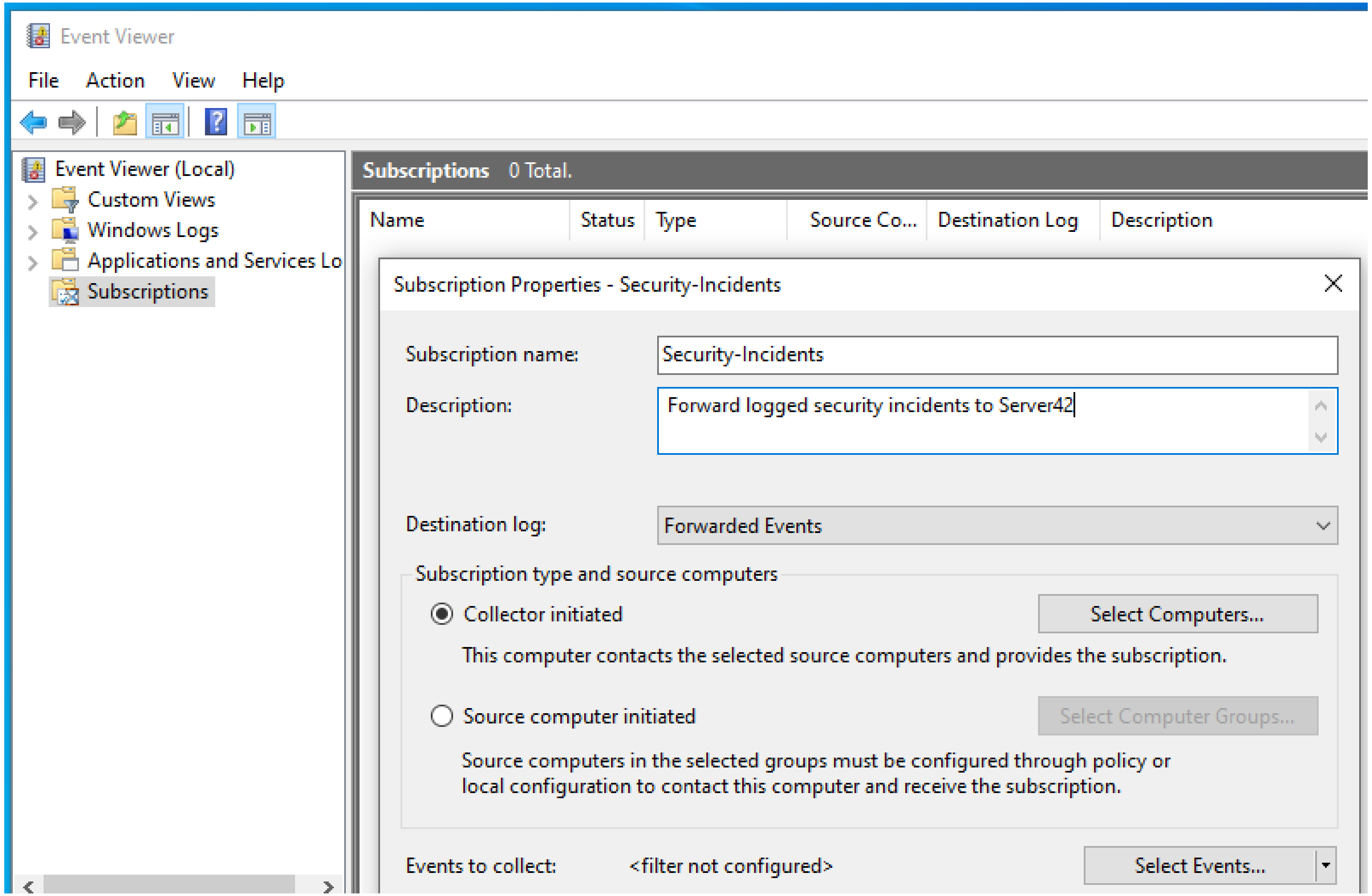
Uses WinRM (Windows Remote Management)

You configure a Windows server to be the “collector”

Then you configure Windows servers and clients to be subscribers (forward select events)

HTTP on TCP 5985

Windows Event Log Subscription Example



Subscriptions 0 Total.

Name	Status	Type	Source Co...	Destination Log	Description

Subscription Properties - Security-Incidents

Subscription name: Security-Incidents

Description: Forward logged security incidents to Server42

Destination log: Forwarded Events

Subscription type and source computers

● Collector initiated

This computer contacts the selected source computers and provides the subscription.

○ Source computer initiated

Source computers in the selected groups must be configured through policy or local configuration to contact this computer and receive the subscription.

Events to collect: <filter not configured>

Simple Network Management Protocol (SNMP)

Used to monitor and manage network-connected devices in an IP network

- Queries devices on a regular interval (typically every 5 minutes)

Does not require the device to maintain its own log

this is the software

Does require the device to be able to answer the queries

Most network devices include an SMNP agent that responds to SNMP manager queries

The manager must identify itself as belonging to the same “community” as the agent

Different community strings can be used for different privilege levels

- “public” is the default string for reading information
- “private” is the default string for reading and writing/configuring

SNMP (cont’d)

Agents can be configured to immediately send an alert (trap) to the manager if a specific event occurs

provides a common mechanism for network devices to relay management information within single and multi-vendor LAN or WAN environments

UDP 161 and 162

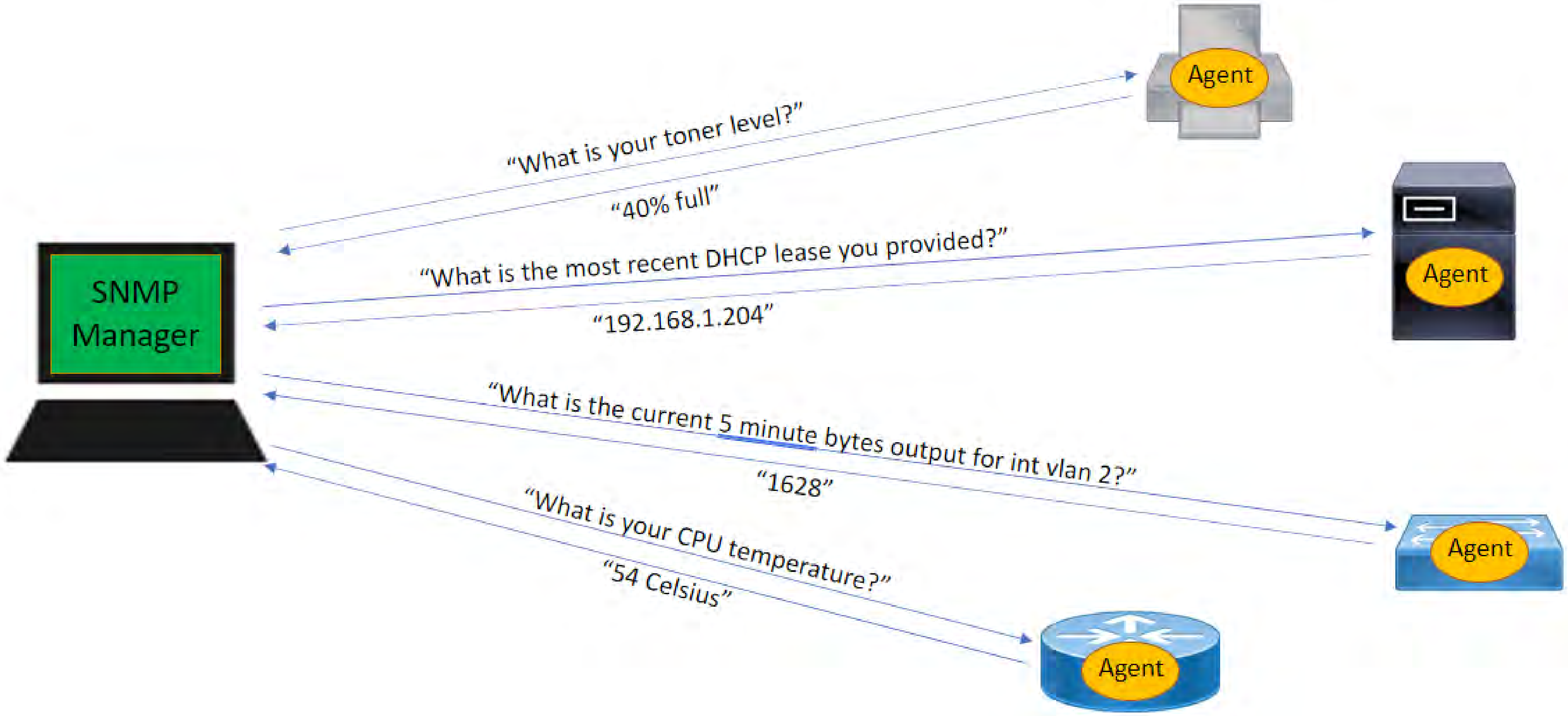
Common versions include v1, v2c, and v3

Only v3 is encrypted

Basic SNMP Commands

Command	Description
Get	Retrieve a value for a specific OID
Get-next	Retrieve the value of the next OID on the device Manager does not need to know what this OID is
Get-bulk	Get all values (bulk data) from a MIB table
set	Modify or assign a value on the agent

SNMP Example


SNMP Manager
Agent
"What is your toner level?"
"40% full"
Agent
"What is the most recent DHCP lease you provided?"
"192.168.1.204"
"What is the current 5 minute bytes output for int vlan 2?"
"1628"
Agent
"What is your CPU temperature?"
"54 Celsius"
Agent

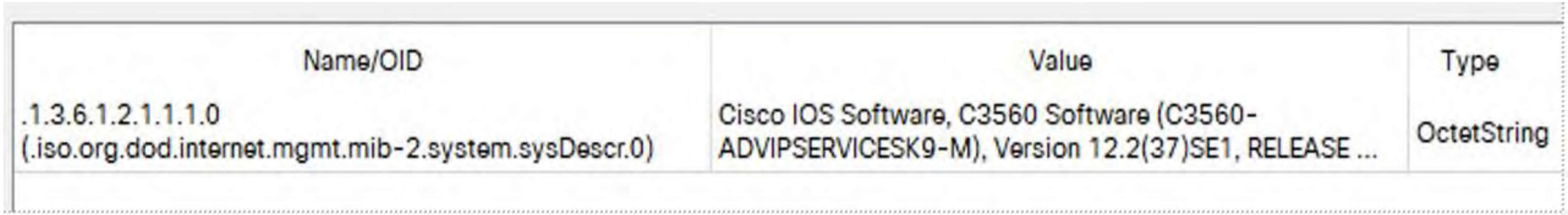
Object Identifier (OID)

Represents a “question” an SMNP manager can ask an agent

Identifies a very specific counter on a device

Has a corresponding name and data type

When queried by manager, agent will return a value



Name/OID	Value	Type
.1.3.6.1.2.1.1.1.0 (.iso.org.dod.internet.mgmt.mib-2.system.sysDescr.0)	Cisco IOS Software, C3560 Software (C3560-ADVIPSERVICESK9-M), Version 12.2(37)SE1, RELEASE ...	OctetString

Management Information Base (MIB)

Hierarchical collection of OIDs

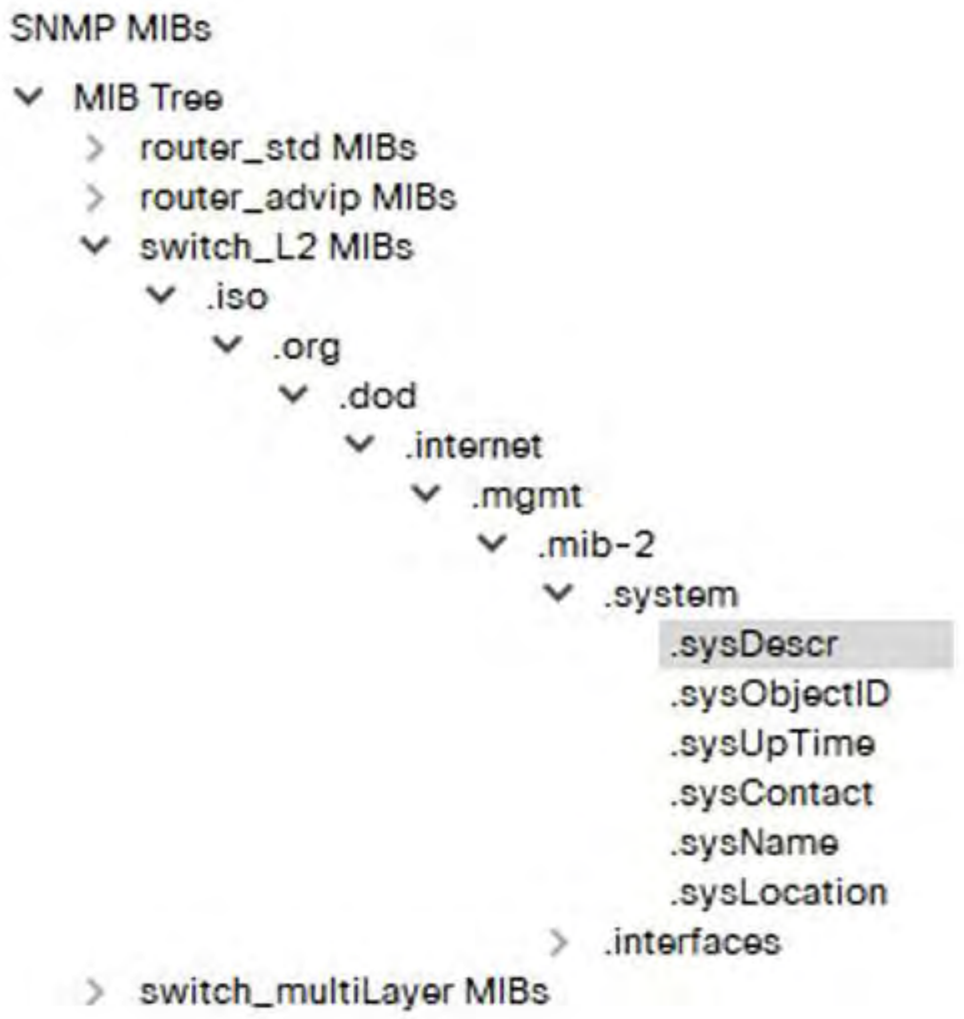
Ensures counter uniqueness

MIBs can be vendor neutral or specific to a product

An agent might use multiple MIBs

SNMP manager must know what MIBs the agent is using

- Or at least know a starting OID to query



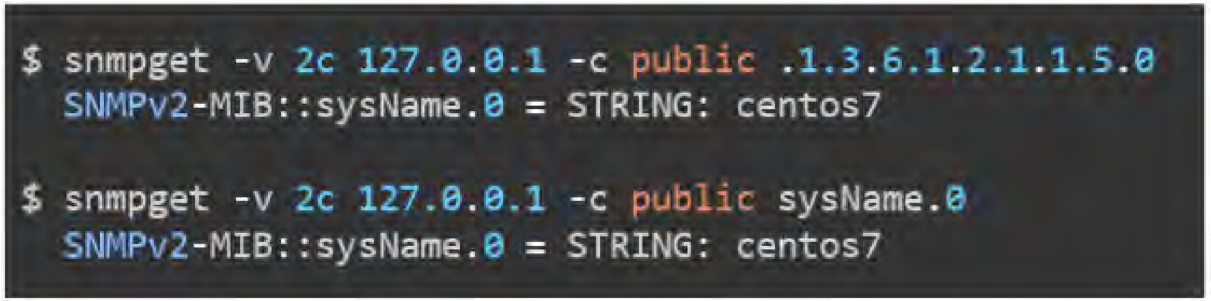
SNMP MIBs

- MIB Tree
  - router_std MIBs
  - router_advip MIBs
  - switch_L2 MIBs
    - .iso
      - .org
        - .dod
          - .internet
            - .mgmt
              - .mib-2
                - .system
                  - .sysDescr
                  - .sysObjectID
                  - .sysUpTime
                  - .sysContact
                  - .sysName
                  - .sysLocation
                - .interfaces
  - switch_multiLayer MIBs

SNMP Manager Examples

Command-line tools

- snmpget
- snmpwalk

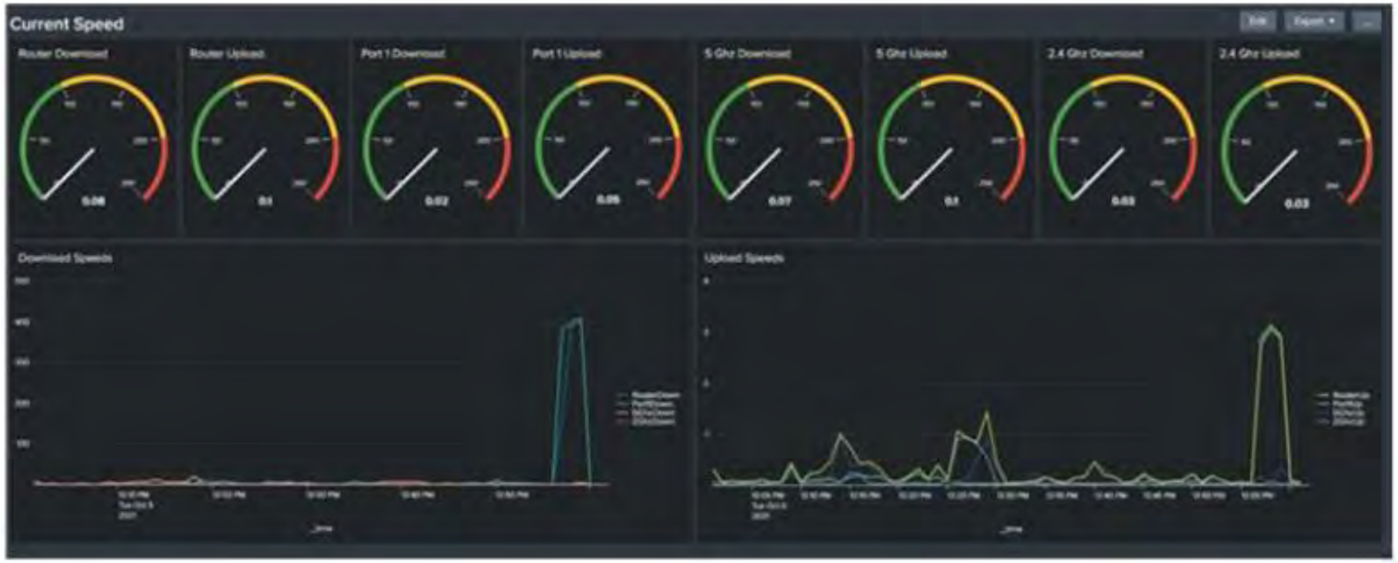


```
$ snmpget -v 2c 127.0.0.1 -c public .1.3.6.1.2.1.1.5.0
  SNMPv2-MIB::sysName.0 = STRING: centos7

$ snmpget -v 2c 127.0.0.1 -c public sysName.0
  SNMPv2-MIB::sysName.0 = STRING: centos7
```

Graphical open source or third party tools

- Paessler PRTG
- Solar Winds
- Splunk
- Observium
- Nagios


Current Speed
Edit
Export
Router Download
Router Upload
Port 1 Download
Port 1 Upload
5 Ghz Download
5 Ghz Upload
2.4 Ghz Download
2.4 Ghz Upload
0.08
0.1
0.02
0.05
0.07
0.1
0.03
0.03
Download Speeds
Upload Speeds