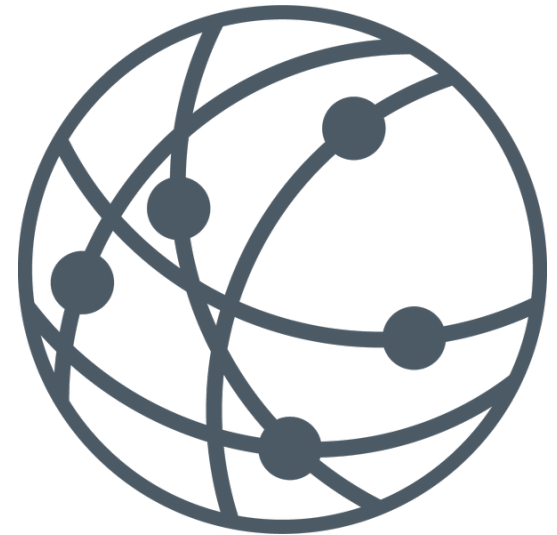


# Internet Connections

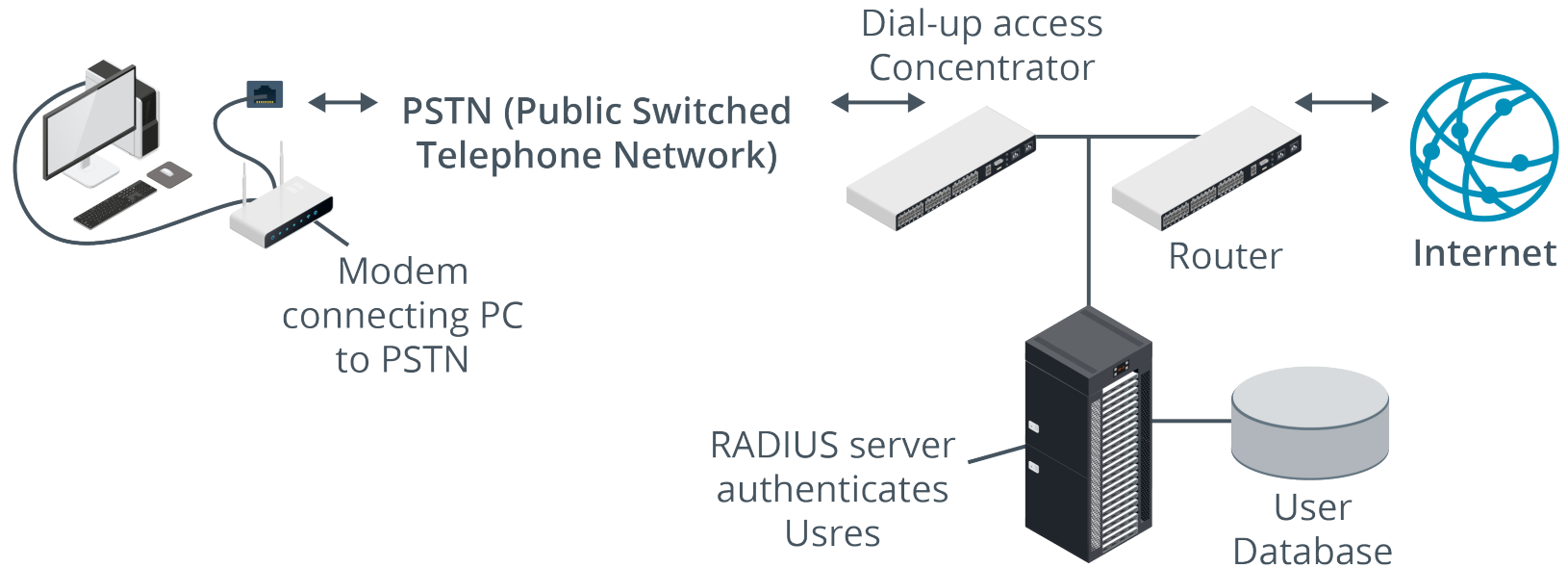
- Businesses and homes depend on Internet access.
- Internet backbone: high-bandwidth backbones connecting Internet eXchange Points (IXPs).
- Created by telecommunications companies and academic institutions .
  - Organized nationally and internationally.



# Internet Service Providers (Slide 1 of 2)

- Home and business networks use ISP to connect to Internet.
  - Network connects to ISP's Point of Presence (PoP).
  - Dial-up, broadband (DSL, FTTx, cable), wireless connections.
  - Most use PSTN (aka POTS, "local loop," "last mile").
- ISP allocates IP addresses, registers domain names, hosts email and websites.
- Enterprise ISPs offer high bandwidth through fiber optic cable.

# Internet Service Providers (Slide 2 of 2)



# Broadband Internet Access

- A range of technologies
- “Always on”
- Data transfer rates much higher than dial-up

# DSL (Slide 1 of 2)

- DSL uses high frequencies in digital phone line for communications.
- Filter separates DSL signals from voice traffic.
- Advanced modulation and echo cancelling enable high-bandwidth, full-duplex.
- DSL “modem” connects to phone system (usually router/modem/AP appliance).
- Phone line connects to DSL modem bank (DSLAM).
- PPP over ATM (PPPoA) or PPP over Ethernet (PPPoE).

# DSL (Slide 2 of 2)

DSL Type	Description
<b>Asymmetrical DSL (ADSL)</b>	<ul style="list-style-type: none"><li>• Consumer version; fast downlink, slow uplink</li><li>• Various iterations</li><li>• ADSL2+: downlink rates up to ~24 Mbps; uplink rates up to ~1.4 Mbps</li><li>• Providers may restrict data download</li><li>• Cable quality, number of users may affect speed</li><li>• Max range ~2 miles/3 km</li></ul>
<b>Symmetric DSL</b>	<ul style="list-style-type: none"><li>• Same uplink and downlink speeds</li><li>• Useful for businesses, branch offices</li></ul>
<b>Very High Bitrate DSL (VDSL)</b>	<ul style="list-style-type: none"><li>• High bit rate at expense of range</li><li>• Symmetric and asymmetric modes</li><li>• Asymmetric: 52 Mbps downstream/6 Mbps upstream over 300 m/1000 ft</li><li>• Symmetric: 26 Mbps in both directions</li><li>• VDSL2: 100 Mbps bi-directional rate for very short range</li></ul>

# Fiber Optic Internet Access (Slide 1 of 3)

- Higher bandwidth, longer distance than copper cable
- Has replaced copper as core of telecommunications networks
- Being extended to individual homes and businesses
- Two principal types of fiber optic network services:
  - Cable TV providers
  - Telecom providers

# Fiber Optic Internet Access (Slide 2 of 3)

- Hybrid Fiber Coax (HFC)/Cable (“broadband cable” “cable”): Connection through CATV service, combines fiber core with coax to customer.
- Cable modem connects to local network through Ethernet adapter.
- Coax links all premises in a street with CMTS to ISP PoP via fiber backbone.
- DOCSIS: Downlink up to 38 Mbps (North America) or 50 Mbps (Europe); and uplink up to 27 Mbps.
- DOCSIS v3 allows multiplexed channels for higher bandwidth.

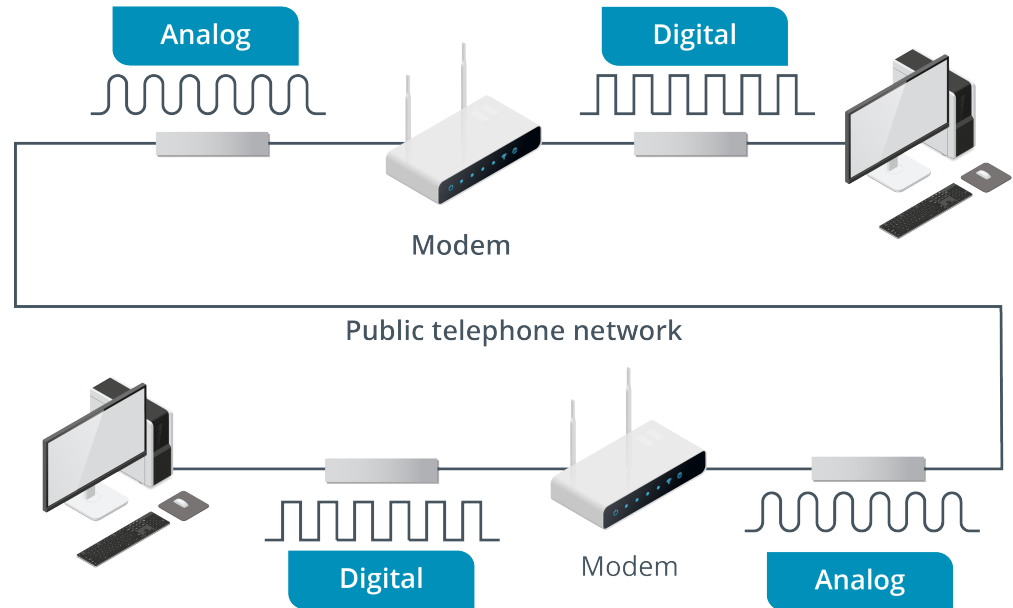


# Fiber Optic Internet Access (Slide 3 of 3)

FTTx Solution	Description
<b>Fiber to the X (FTTx)</b>	<ul style="list-style-type: none"><li>• Solutions where fiber replaces copper in the “last mile”</li></ul>
<b>Fiber to the Premises (FTTP)</b> <b>Fiber to the Home (FTTH)</b>	<ul style="list-style-type: none"><li>• Most expensive, not widespread</li><li>• Fiber link terminated at customer premises equipment</li></ul>
<b>Fiber to the Node (FTTN)</b> <b>Fiber to the Curb/Cabinet (FTTC)</b>	<ul style="list-style-type: none"><li>• Fiber to communications cabinet at street</li><li>• Similar to HFC, but consumer link uses VDSL over phone wiring (not coax)</li></ul>

# Dial-Up Internet Access (Slide 1 of 2)

- Telephone connection between computers.
- Uses entire frequency range; not efficient, low bandwidth.
- Phone charges apply; line cannot be used for voice at same time.
- Modems at each end convert digital  $\leftrightarrow$  analog (MOdulation/DEModulation).



# Dial-Up Internet Access (Slide 2 of 2)

- Disadvantages: low data transfer, time to establish connection, errors
- Fastest modems ~33.6 Kpbs; speed limit of phone line
- Theoretical maximum downlink ~56 Kpbs
- Compression may improve data transfer
- Has been superseded; still in use as a backup or for areas without other support

# ISDN Internet Access

- Digital circuit-switched technology for voice, video, data.
- Uses copper telephone wiring if of sufficient quality.
- Uses digital signatures for both voice and data; no analog conversions.
- Dial-up service billed by line rental and usage; establishes connection in ~1 second.
- Used to connect LANs and for remote workers.
- Two classes:
  - BRI: two 64 Kbps "B" data channels for data and one 16 Kbps "D" control channel.
  - PRI: 23 or 30 "B" channels, one 24 Kbps "D" channel.
- Remains in use for telecom core; superseded by DSL/cable for subscribers.
- Terminal Adapter connects to PC or router; to network via NT1 device.

# Fixed Wireless Internet Access (Slide 1 of 2)

- Wired broadband may not be available:
  - In rural areas
  - In older buildings where not possible to run new cable
- Fixed wireless may be an option
- Two options:
  - Satellite
  - Line of Sight (LoS) Wireless Internet Provider (WISP)

# Fixed Wireless Internet Access (Slide 2 of 2)

Solution	Description
<b>Satellite</b>	<ul style="list-style-type: none"><li>• Large coverage area with VSAT microwave antenna aligned to orbital satellite.</li><li>• Super High Frequency range (3-30 GHz).</li><li>• Satellite television receivers for domestic use; use growing for businesses, especially rural.</li><li>• Transfer rates vary: 6 Mbps / 15-20 Mbps down typical.</li><li>• Can be severe latency problems.</li><li>• Dish at customer aligned with satellite; connects via coax to DVB-S modem.</li></ul>
<b>LoS WISP</b>	<ul style="list-style-type: none"><li>• Ground-based microwave antennas aligned with each other; transmit if no physical obstruction (usually atop tall buildings).</li><li>• Spans great distances; no cabling infrastructure; lower latency than satellite.</li><li>• Hard to maintain line of sight; expensive.</li><li>• WISP may use Wi-Fi or proprietary equipment.</li><li>• Range of frequencies; may be affected by 5G cellular phone service deployment.</li></ul>

# Cellular Radio Networks (Slide 1 of 2)

- Wi-Fi bands have restricted range; fixed wireless requires large antenna.
- Cellular radio wireless networking allows long-distance communications over smartphone devices.
- Also used by IoT devices.
- Connects to nearest transmitter; base station range of up to 5 miles.
- Transmitter connects phone to mobile/landline networks.
- 850 / 1900 MHz bands (Americas); 900 / 1800 MHz bands (rest of world).

# Cellular Radio Networks (Slide 2 of 2)

Generation	Description
<b>2G</b>	<ul style="list-style-type: none"><li>• GSM phones using a SIM card; international, and AT&amp;T in US</li><li>• TIA/EIA IS-95 (cdmaOne) handsets managed by provider with CDMA; Sprint and Verizon</li><li>• Data access built on top of existing voice network using CSD</li><li>• Must establish data connection to base station, incurring charges; maximum ~14.4 Kpbs</li></ul>
<b>3G</b>	<ul style="list-style-type: none"><li>• Deployed packet-switched technology to mobiles</li><li>• GPRS/EDGE; HSPA+; CDMA2000/Evolution Data Optimized (EV-DO)</li></ul>
<b>4G</b>	<ul style="list-style-type: none"><li>• LTE: converged 4G standard supported by all network providers, requires a SIM. Maximum 150 Mbps down; 20 Mbps real-world</li><li>• LTE-A: Intended to provide 300 Mbps down; 40 Mbps current real-world</li></ul>
<b>5G</b>	<ul style="list-style-type: none"><li>• Target is for 1 Gbps if stationary or slow-moving; 100 Mbps if fast-moving</li><li>• Available in trial areas; commercially in ~2020</li><li>• 70 Gpbs in test conditions (<i>← James is this right???? Should this be 70 Mbps? –LO</i>)</li></ul>



# Activity



# Routers (Slide 1 of 2)

- Switches use MAC addresses; routers use logical network and host IDs.
- Many different types and uses; two general tasks:
  - LAN router: divides a physical network into logical networks.
  - WAN (edge/border) router: joins separate networks (i.e.; LAN to Internet).
- Route/path to destination is selected either dynamically or statically; packet moves by hops along path to target.
- At target, hardware address determines destination node.



# Routers (Slide 2 of 2)

- Routers and modems both connect to the Internet:
  - Modem makes a physical link (like a switch).
  - Router makes logical forwarding decisions.
  - Often bundled in one device.
- Switched enterprise networks can have thousands of ports; inefficient to treat as one logical network.
  - Use VLANs on managed switches to group ports into logical subnets.
  - VLANs communicate through routers.
  - Also provides filtering and monitoring to improve security.

# The TCP/IP Protocol Suite (Slide 1 of 3)



**Protocol:** Rules and formats enabling systems to exchange data.

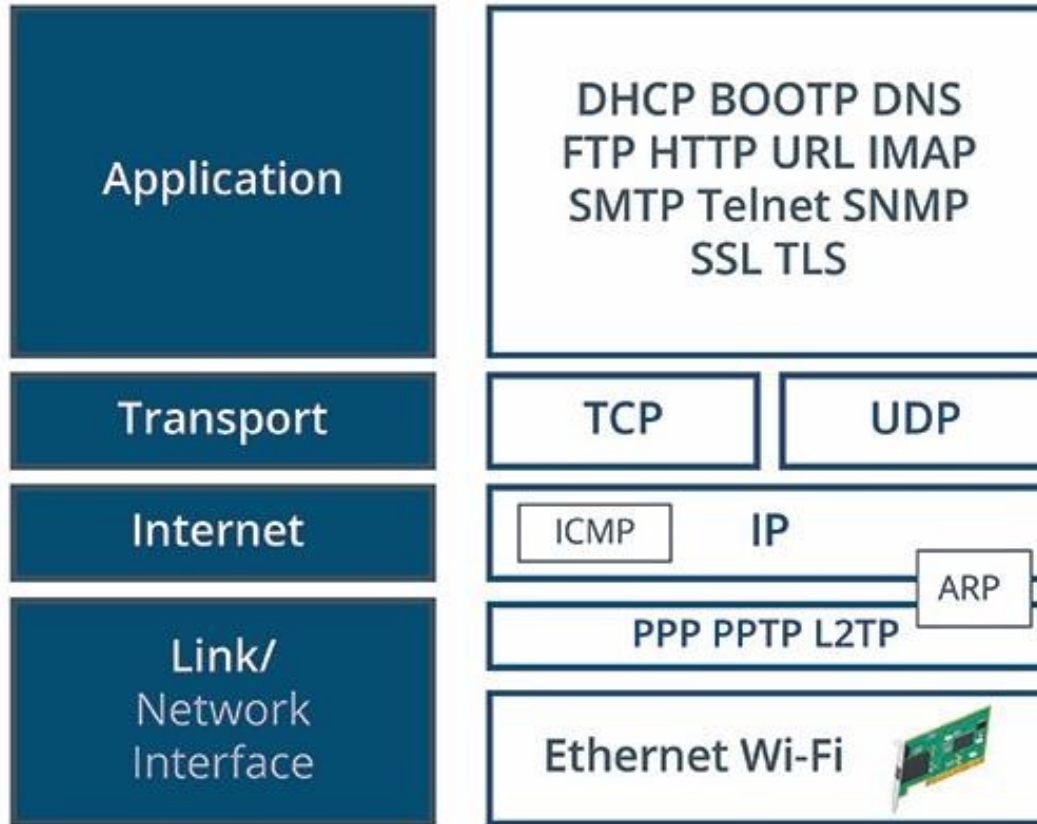
**Protocol Suite:** A collection of several protocols used for networking are designed to work together.

- Networks have converged on use of TCP/IP protocol suite
- Originally developed by US DoD; now an open standard
- IETF working groups implement development
- RFCs are published standards
- Packet-based protocols
- Routers select the path for packets
- Main protocols handle addressing and transport
- Divided into four-layer model

# The TCP/IP Protocol Suite (Slide 2 of 3)

Layer	Description
<b>Link/Network Interface Layer</b>	<ul style="list-style-type: none"><li>• Puts frames on physical network</li><li>• Not TCP/IP protocols as such; networking products and media (Ethernet, Wi-Fi)</li><li>• Communications on local network</li><li>• Data packaged in frames</li><li>• Nodes identified by MAC address</li></ul>
<b>Network Layer (IP Protocol)</b>	<ul style="list-style-type: none"><li>• IP provides packet addressing and routing</li><li>• Best-effort delivery; unreliable, connectionless</li></ul>
<b>Transport Layer (TCP/UDP Protocols)</b>	<ul style="list-style-type: none"><li>• TCP guarantees orderly packet transmission</li><li>• UDP provides non-guaranteed packet transfer, but is faster</li></ul>
<b>Application Layer</b>	<ul style="list-style-type: none"><li>• Numerous protocols for network configuration, management, services; use TCP/UDP ports</li><li>• ARP: Finds MAC address associated with IP address</li><li>• ICMP: delivers status and error messages (used by ping and tracert)</li></ul>

# The TCP/IP Protocol Suite (Slide 3 of 3)



# Internet Protocol and IP Addressing (Slide 1 of 4)

- Two versions of IP, IPv4 and IPv6. Main headers in IPv4.

IPv4 Frame Field	Description
<b>Source IP Address</b>	Identifies the sender of the datagram by IP address.
<b>Destination IP Address</b>	Identifies the destination of the datagram by IP address.
<b>Protocol</b>	Indicates whether data should be passed to TCP or UDP at the destination.
<b>Checksum</b>	Verifies the packet's integrity at the destination.
<b>Time to Live</b>	<ul style="list-style-type: none"><li>• The number of hops the datagram can stay on the network before it is discarded; avoids endless looping of undeliverable packets.</li><li>• Each router decreases the TTL value by at least one.</li></ul>

# Internet Protocol and IP Addressing (Slide 2 of 4)

- IP address defines source and destination of packet:

32 binary digits:

11000110001010010001000000001001

Divided into octets:

11000110 00101001 00010000 00001001

Converted to dotted-decimal notation:

198 . 41 . 16 . 9



# Internet Protocol and IP Addressing (Slide 3 of 4)

- In binary, a digit can only be 0 or 1
- Values of the digits are powers of 2
- Converting 11101101 from binary to decimal:

Place value:	128	64	32	16	8	4	2	1
Binary value:	1	1	1	0	1	1	0	1
Conversion:	$128*1$	$64*1$	$32*1$	$16*0$	$8*1$	$4*1$	$2*0$	$1*1$
Decimal equivalent:	$128 + 64 + 32 + 0 + 8 + 4 + 0 + 1 = 237$							

# Internet Protocol and IP Addressing (Slide 4 of 4)

- Converting 199 from decimal to binary:

199 =

Decimal value:	128	+	64	+	0	+	0	+	0	+	4	+	2	+	1
Place value:	128		64		32		16		8		4		2		1
Conversion:	128*1		64*1		32*0		16*0		8*0		4*1		2*1		1*1
Binary equivalent:	1		1		0		0		0		1		1		1

- Maximum value of a byte is 255, minimum is 0.
- Theoretical address range is 0.0.0.0 to 255.255.255.255; some addresses not permitted or reserved.

# Subnet Masks (Slide 1 of 4)

- IP address encodes both network ID and host ID.
- Subnet mask separates them by “masking” the host from you. Generally you only see the network instead of the actual devices.
- Binary 1 in the mask = address digit is part of network ID.
- Size of the network portion of the subnet mask determines how many networks and hosts allowed in a given addressing scheme.
- Expressed in dotted decimal or as network prefix (contiguous number of 1s in the mask).

# Subnet Masks (Slide 2 of 4)

- Default masks and network classes (note: network prefix is the number of hosts hidden inside a network mask):

Class	Dotted Decimal Mask	Network Prefix	Binary Mask
<b>A</b>	255.0.0.0	/8	11111111 00000000 00000000 00000000
<b>B</b>	255.255.0.0	/16	11111111 11111111 00000000 00000000
<b>C</b>	255.255.255.0	/24	11111111 11111111 11111111 00000000

# Subnet Masks (Slide 3 of 4)

- Network ID revealed by “ANDing”
- 1 AND 1 = 1; all other combinations = 0
- Example:

172.	30.	15.	12	10101100	00011110	00001111	00001100
255.	255.	0.	0	11111111	11111111	00000000	00000000
172.	30.	0.	0	10101100	00011110	00000000	00000000

# Subnet Masks (Slide 4 of 4)

- Hosts communicate directly if on same network
- IP protocol uses subnet mask to compare source/destination network ID
- If on same network, delivers locally:

172. 30. 15. 12

255. 255. 0. 0.

- Top mask address and bottom match,
- same network so local delivery.

172.	30.	16.	101
------	-----	-----	-----

- If on different network, sends to router:

172. 30. 15. 12

255. 255. 0. 0.

172.	31.	16.	101
------	-----	-----	-----

# Host IP Configuration

- Host must have IP address and subnet mask; should have other parameters for proper network/Internet communication.

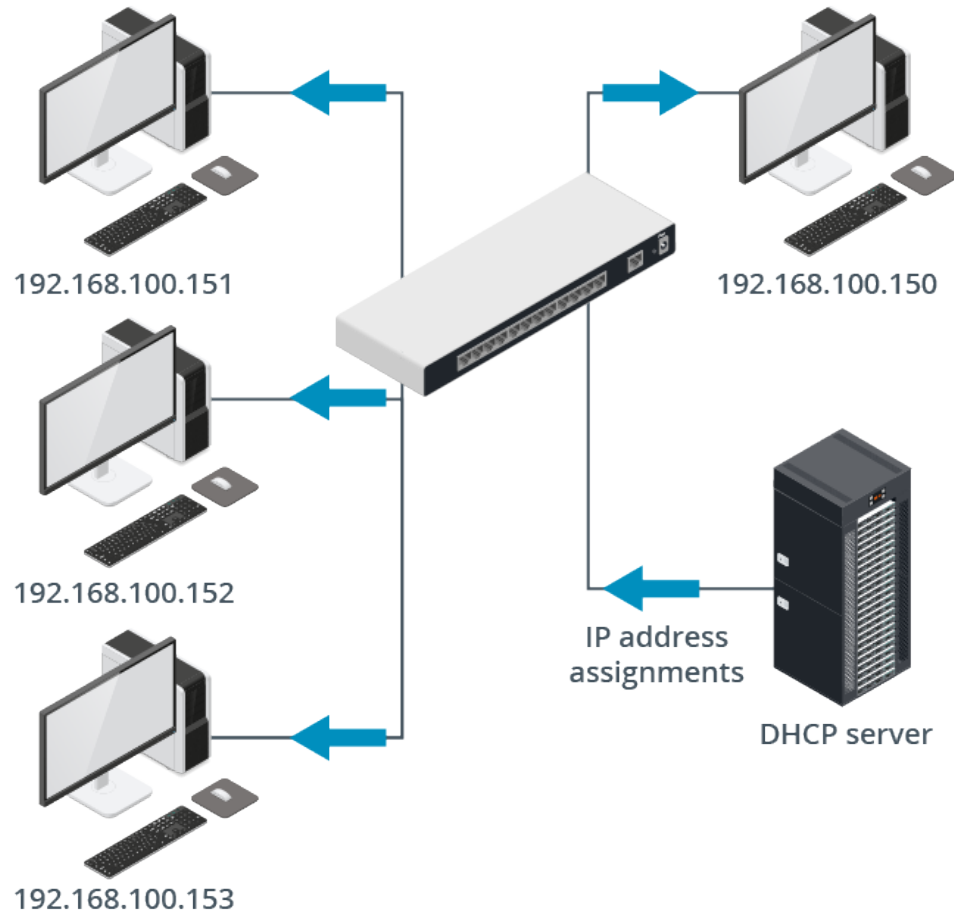
Parameter	Description
<b>IPv4 address</b> <b>Subnet mask</b>	<ul style="list-style-type: none"><li>• Both required for every interface; can be set manually.</li><li>• Address: dotted-decimal notation; identifies host and network.</li><li>• Subnet mask determines if other hosts are local or remote.</li></ul>
<b>Default gateway</b>	<ul style="list-style-type: none"><li>• IP address of a router to send packets outside of local network.</li><li>• If no gateway, host can only communicate on local network.</li></ul>
<b>Client DNS</b>	<ul style="list-style-type: none"><li>• IP address of DNS server to provide host/domain name resolution and locate Internet resources.</li><li>• DNS also used on most local networks.</li><li>• Often the gateway address; often a second server address provided for redundancy.</li></ul>

# Static and Dynamic IP Addresses (Slide 1 of 3)

- Static addressing:
  - Administrator manually configures each host.
  - Must update manually if host changes subnet.
  - Must track address allocations to avoid duplication.
  - Can be time consuming and error-prone.
  - Only used for systems with dedicated functionality.
- Dynamic addressing:
  - DHCP server allocates addresses.



# Static and Dynamic IP Addresses (Slide 2 of 3)



# Static and Dynamic IP Addresses (Slide 3 of 3)

Dynamic Addressing Method	Description
<b>DHCP</b>	<ul style="list-style-type: none"><li>• DHCP client contacts server on boot and requests address.</li><li>• Also provides other parameters (subnet mask, default gateway) .</li><li>• Limited time leases.</li><li>• Information configured on server; client updated when lease renewed.</li></ul>
<b>Link local APIPA</b>	<ul style="list-style-type: none"><li>• Fallback mechanism for DHCP client if DHCP server is unavailable.</li><li>• Host self-configures with address on 169.254.x.x network.</li><li>• “Link local” is generic term; “APIPA” is Microsoft term.</li><li>• Communication with other APIPA hosts on same network only.</li></ul>
<b>DHCP reservation</b>	<ul style="list-style-type: none"><li>• For hosts that need same address each time.</li><li>• Configure DHCP server with reserved host address per MAC address.</li><li>• Centralized, easier to implement than static addressing.</li></ul>

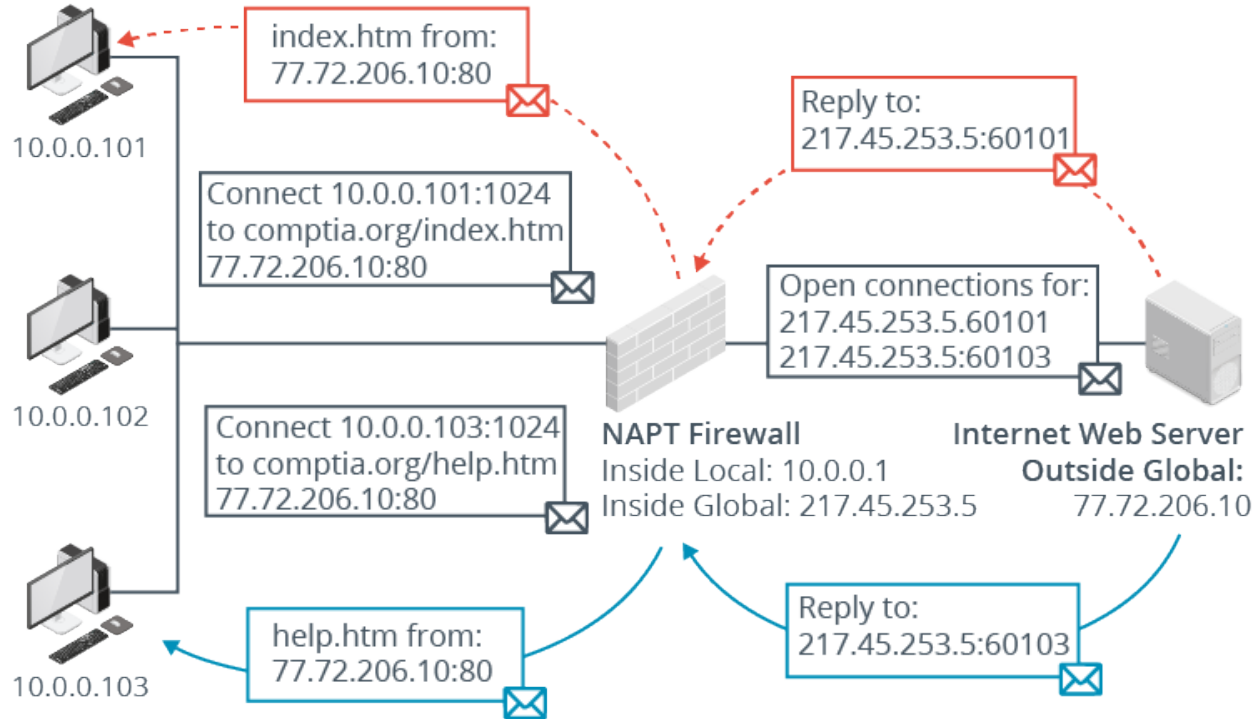
# Public and Private IP Addresses (Slide 1 of 4)

- On the Internet, each host address must be unique; usually allocated by ISP.
- Few organizations have enough individual addresses; various methods to overcome this issue.
- Internal hosts can use addresses in a Class A, B, or C private range defined by RFC 1918 (10.0.0.0 to 10.255.255.255; 172.16.0.0 to 172.31.255.255; 192.168.0.0 to 192.168.255.255).
- Internet access provided for private-address hosts through:
  - A router using NAT.
  - A proxy server.

# Public and Private IP Addresses (Slide 2 of 4)

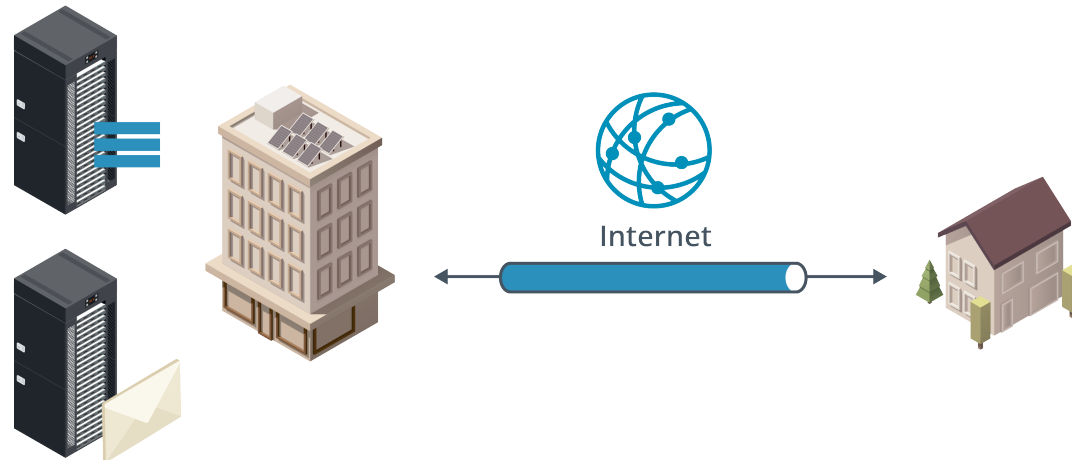
- In NAT, router converts the internal private IP address to a valid public address.
- IP configuration is simpler and internal clients are not directly accessible from the Internet.
- NAT address pool itself will be limited; multiple private addresses will use a single public address.
- Mapping provided by NAT, aka PAT, aka NAT overloading.
  - Each outgoing connection assigned TCP or UDP port.
  - Returning traffic mapped back to address/client port.

# Public and Private IP Addresses (Slide 3 of 4)



# Public and Private IP Addresses (Slide 4 of 4)

- VPN: connects two private networks over a public network (the Internet).
- Internet is cost-effective way to connect users and networks, but is not private.
- VPN protocols create tunnels through the public network to authenticate, encrypt, and secure private communications.



# IPv6 (Slide 1 of 5)

- IPv4 address pool is large, but limited.
- IPv6 uses 128-bit addresses, massively increasing address pool.
- Other improvements: simplified address headers, hierarchical addressing, support for time-sensitive traffic, new unicast address structure.
- Large string of characters in binary or even decimal; affects clarity and accuracy.
- Uses hexadecimal notation (0-9, A-F):

Decimal	Hex	Binary
0	0	0000
1	1	0001
...	...	...
10	A	1010
11	B	1011
...	...	...

## IPv6 (Slide 2 of 5)

- Binary IPv6 address divided into eight double-byte values using hex notation:  
2001:0db8:0000:0000:0abc:0000:def0:1234
- Leading zeros can be ignored, and a contiguous series of zeroes can be replaced by a double colon place marker:

2001:db8::abc:0:def0:1234



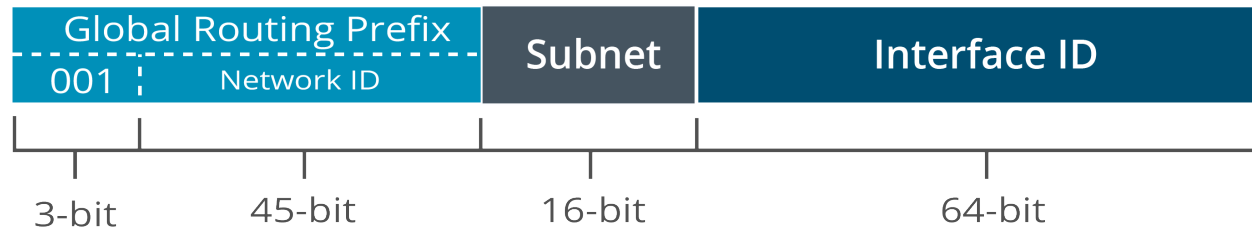
# IPv6 (Slide 3 of 5)

- First 64 bits are network ID, second 64 bits designate the interface
- Fixed size = no subnet mask; /nn = length of routing prefix in bits



# IPv6 (Slide 4 of 5)

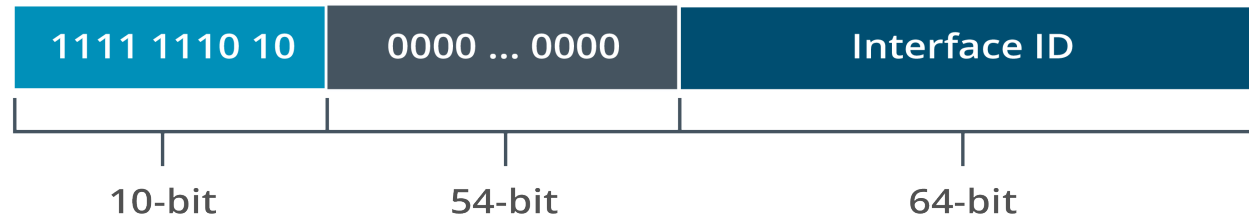
- IPv6 global unicast address format:



- IPv6 address blocks assigned hierarchically by routers; logical address space

# IPv6 (Slide 5 of 5)

- IPv6 link-local addresses used for housekeeping
- Span single subnet
- Nodes on same link called “neighbors”
- Start with fe80::
- Equivalent of APIPA
- IPv6 host always has a link-local address



# Activity



Discussing Network Configuration Concepts

30bird 13.11, 13.1.2, 13.1.3, 13.1.5

# TCP and UDP Ports (Slide 1 of 2)

- Transport-layer protocols ensure effective delivery; content of packets is significant.
- Identifies network application types by assigning port number (0-65535).
- Data from upper layers is packaged in segments, tagged with port number.
- Passed to network layer for delivery.
- Simultaneous segment transmissions are multiplexed onto network link; de-multiplexed at receiving host.
- Can use TCP or UDP.

# TCP and UDP Ports (Slide 2 of 2)

Port Type	Description
<b>TCP</b>	<ul style="list-style-type: none"><li>• Ensures reliability and sequencing with acknowledgement messages.</li><li>• If non-delivery, retransmits if lack of acknowledgement.</li><li>• If damaged delivery, NACK forces retransmission.</li><li>• Connection-oriented.</li><li>• Acknowledgements add overhead, slow communications.</li></ul>
<b>UDP</b>	<ul style="list-style-type: none"><li>• Connectionless, non-guaranteed, no sequencing or flow control.</li><li>• Speeds up communication by reducing overhead.</li><li>• For applications that:<ul style="list-style-type: none"><li>• Don't require acknowledgement and can tolerate missing or out-of-order packets.</li><li>• Are time-sensitive but don't need complete reliability.</li></ul></li></ul>

# Well-Known Ports

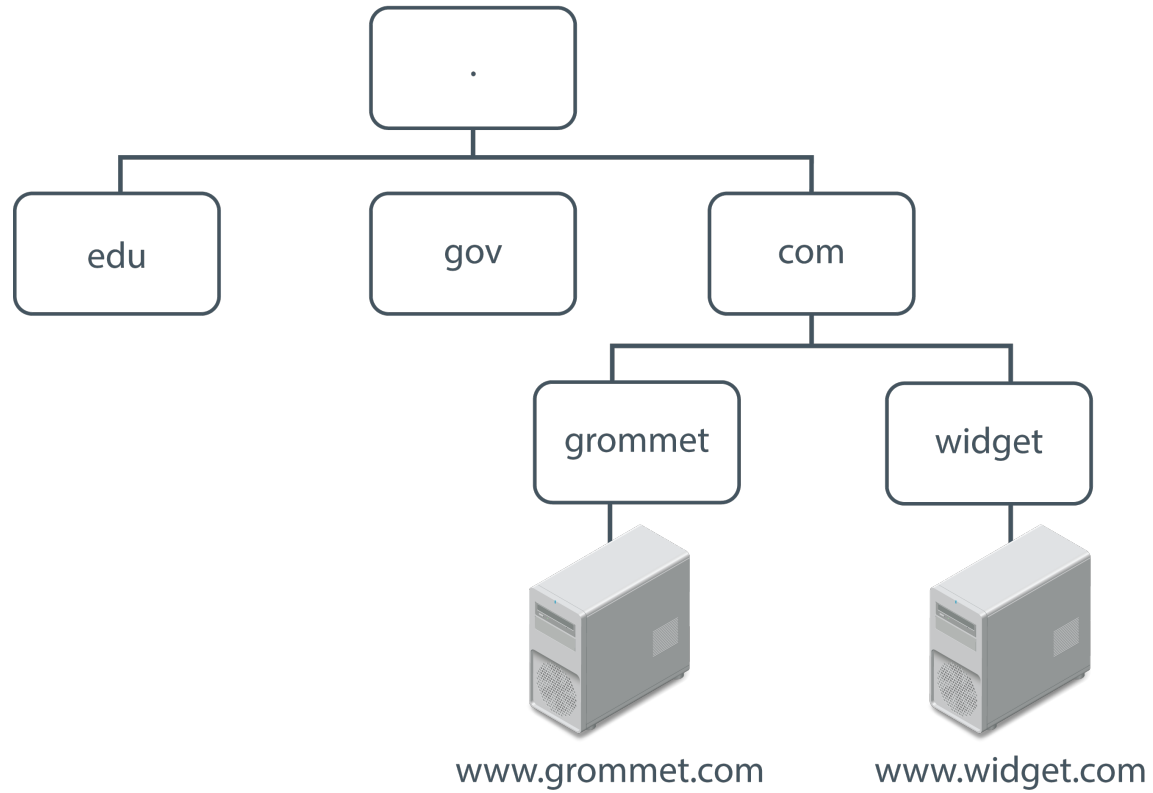
- Port: unique ID for a service using TCP or UDP for transport.
- ID might be persistent (for servers) or ephemeral (for clients).
- IANA assigns standard (“well-known”) port numbers to services.
  - See course text for examples.
- IANA defines ephemeral port range (49152 to 65535); some OSes use different values.
- Firewalls must have ports enabled or disabled to allow only valid traffic.

# DNS (Slide 1 of 4)

- Hierarchical system for resolving names to IP addresses.
- Database distributed among many name servers; distributes maintenance, protects against server loss.
- Root (.) at top; then 13 TLDs (generic, sponsored, or country code); then domains.
- Domain names managed by ICANN, registered with the appropriate Domain Name Registry for the TLD.
- Records traced from root down; each level of server has information about servers below in hierarchy.

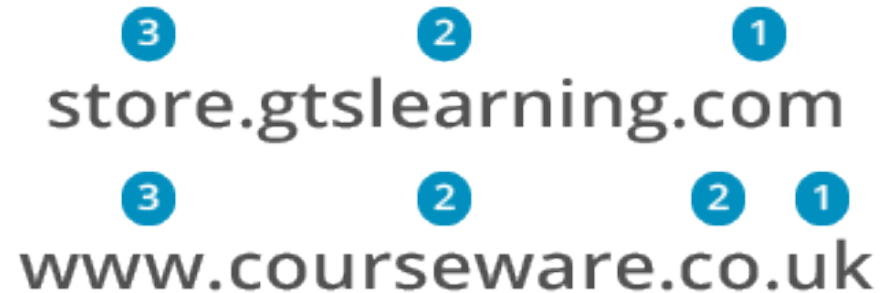


# DNS (Slide 2 of 4)



# DNS (Slide 3 of 4)

- FQDN shows hierarchy from most specific on left to least specific on right.
- Domain name portion identifies the company, organization, or individual; must be unique and officially registered.
- Host name identifies particular server or server alias.



# DNS (Slide 4 of 4)

DNS Server Type	Description
<b>Authoritative name server</b>	<ul style="list-style-type: none"><li>• Holds domain records and can respond authoritatively about hosts in the domains it manages.</li><li>• Required for Active Directory.</li><li>• If private domain, not available outside the LAN; on Internet, published to name servers hosted by ISPs.</li></ul>
<b>Recursive resolver</b>	<ul style="list-style-type: none"><li>• Resolves names for clients.</li><li>• Client contacts resolver; resolver contacts name servers until record is located or request times out.</li><li>• DNS clients are configured with resolver address.</li><li>• Listens on UDP 53.</li></ul>

# Web Servers and HTTP/HTTPS (Slide 1 of 3)



**Web server:** A server that provides client access using HTTP (defaults to port 80) or its secure version HTTPS (defaults to port 443).

- Organizations may lease from ISP; host directly; use private servers (intranets)
- Provides HTML pages (text files with tags), interpreted by browsers
- Extended by scripts and web applications

# Web Servers and HTTP/HTTPS (Slide 2 of 3)

- Uses URL to access resources:
  1. Protocol
  2. FQDN
  3. File path

**1** **2** **3**  
`http://store.gtslearning.com/comptia/index.htm`

# Web Servers and HTTP/HTTPS (Slide 3 of 3)

- HTTP lacks security; data sent unencrypted, no authentication.
- SSL/TLS can be used to encrypt TCP/IP applications that use TCP connections, including HTTPS.
- Servers use digital certificates from Certification Authorities to prove the identity of the server and to provide encryption.



# Mail Servers (Slide 1 of 3)

- Email can send text and file attachments encoded using MIME.
- Can use multiple protocols; typical process:
  1. Client sends message to server; server queues message for an SMTP session (port 25).
  2. SMTP server uses DNS to resolve address of recipient's mail server.
  3. SMTP delivers message; usually several "hops."
  4. Message placed in store on recipient's server; client software connects with mailbox using POP3 (port 110) or IMAP (port 143).
    - POP3 more widely used; IMAP has more features.
- Email account requires username, password, email address, incoming and outgoing server addresses, and protocol types.

# Mail Servers (Slide 2 of 3)

Add Account ✕

**POP and IMAP Account Settings**  
Enter the mail server settings for your account.

**User Information**

Your Name:

Email Address:

**Server Information**

Account Type:  ▼

Incoming mail server:

Outgoing mail server (SMTP):

**Logon Information**

User Name:

Password:

Remember password

Require logon using Secure Password Authentication (SPA)

**Test Account Settings**

We recommend that you test your account to ensure that the entries are correct.

Automatically test account settings when Next is clicked

**Deliver new messages to:**

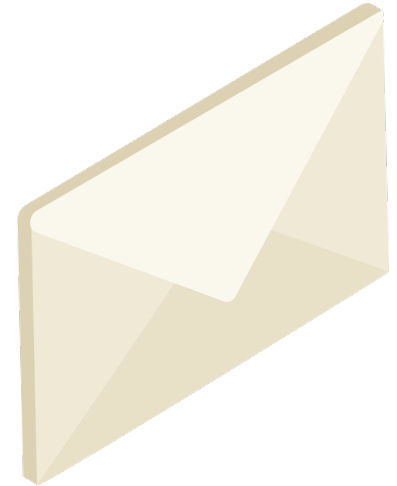
New Outlook Data File

Existing Outlook Data File



# Mail Servers (Slide 3 of 3)

- Mailto URL scheme: username@domainname (domain may be a company or ISP).
- Different systems allow different characters; not usually treated as case sensitive.
- Mail may be rejected if incorrectly addressed, if identified as spam, if mailbox is full.
- Only one of many network communication types.



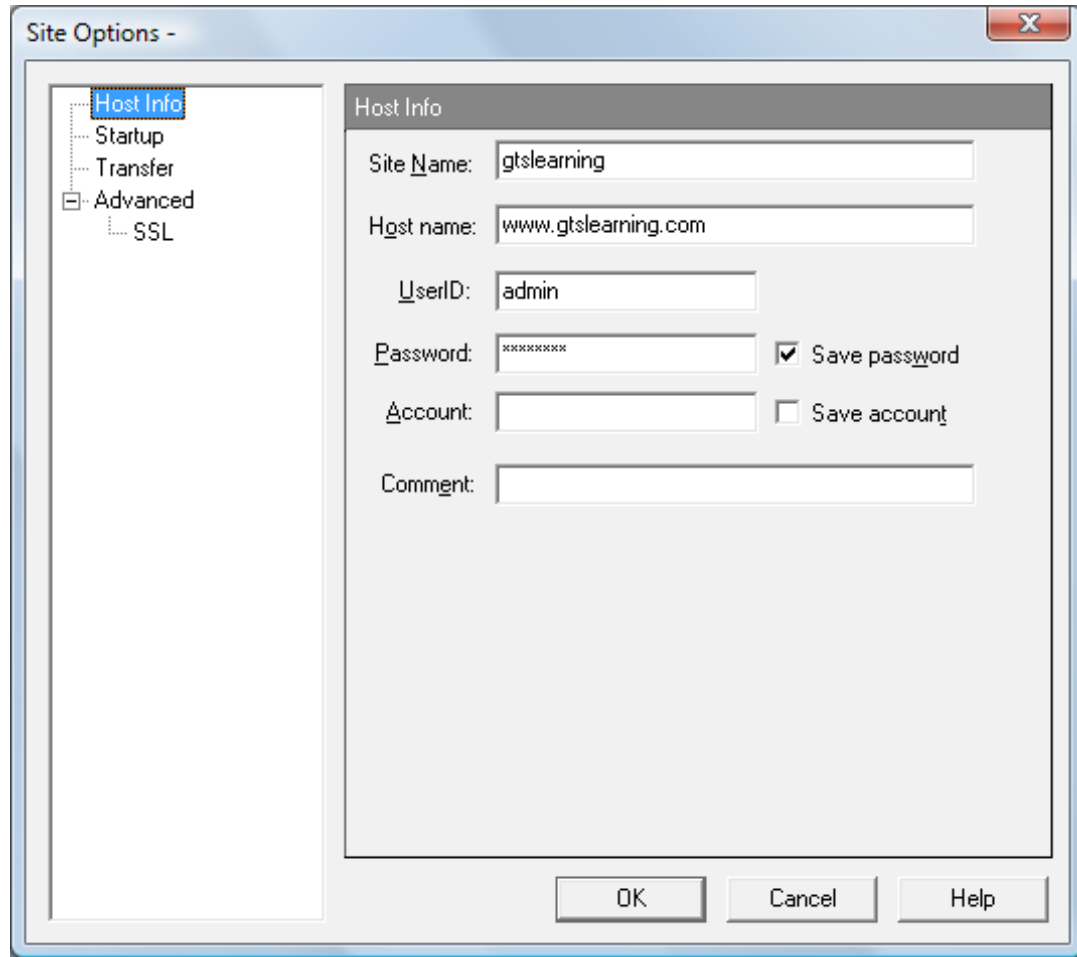
# File and Printer Sharing (Slide 1 of 3)

- Core network functions.
- May be accomplished by proprietary protocols (i.e., File and Print Services for Windows).
- May use standard protocols (i.e., FTP), but may not have as much functionality.

# File and Printer Sharing (Slide 2 of 3)

Protocol	Description
<b>SMB (aka CIFS)</b>	<ul style="list-style-type: none"><li>• Underpins file and printer sharing on Windows networks; currently SMB2, but legacy clients are supported.</li><li>• TCP port 445; also NetBIOS over TCP/IP (UDP and TCP port range 137-139).</li><li>• Implemented as Samba on Linux.</li></ul>
<b>AFP</b>	<ul style="list-style-type: none"><li>• Performs similar function to SMB for Apple/Mac OS.</li><li>• UDP or TCP port 427 (Service Location Protocol)—not required by OS X or later.</li><li>• TCP port 548.</li></ul>
<b>FTP</b>	<ul style="list-style-type: none"><li>• Early TCP/IP protocol; widely used for file transfers; flexible; easy to maintain.</li><li>• TCP port 21 for connection; port 20 for active transfer or server-assigned port if passive.</li><li>• Client options:<ul style="list-style-type: none"><li>• Command line</li><li>• Dedicated GUI</li><li>• Browsers</li></ul></li></ul>

# File and Printer Sharing (Slide 3 of 3)



The screenshot shows a Windows dialog box titled "Site Options -". On the left is a tree view with "Host Info" selected. The main area is titled "Host Info" and contains the following fields and options:

- Site Name: gtslearning
- Host name: www.gtslearning.com
- UserID: admin
- Password: [masked]  Save password
- Account: [empty]  Save account
- Comment: [empty]

At the bottom are buttons for "OK", "Cancel", and "Help".

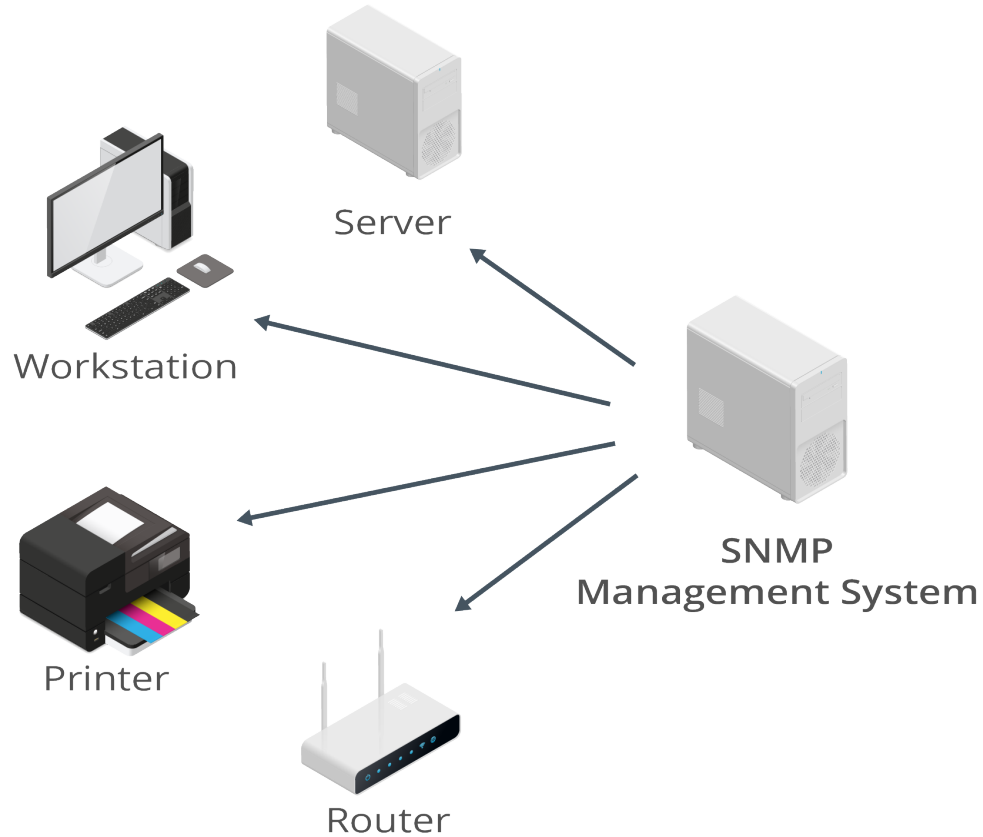
# Network Host Services

Service	Description
<b>Authentication Server</b>	<ul style="list-style-type: none"><li>• Used on enterprise networks to ensure only authorized users can access accounts.</li><li>• On Windows domain, Active Directory provides authentication based on Kerberos.</li><li>• AAA server consolidates authentication across multiple devices.</li><li>• RADIUS is an AAA protocol.</li></ul>
<b>DHCP DNS</b>	<ul style="list-style-type: none"><li>• DHCP assigns IP addresses to hosts when they connect.</li><li>• DNS allows hosts to access resources by host name and FQDN by resolving names to IP.</li></ul>
<b>LDAP</b>	<ul style="list-style-type: none"><li>• Network resources are recorded as objects in a directory database.</li><li>• X.500 standards allow directories to interact; full standard required a complex protocol.</li><li>• LDAP allows X.500-compliant queries and updates over TCP/IP.</li><li>• Widely supported; TCP/UDP 389.</li><li>• Uses Distinguished Names and Relative Distinguished Names as identifiers.</li></ul>
<b>NetBIOS/NetBT</b>	<ul style="list-style-type: none"><li>• NetBIOS first Windows network software; provided name discovery, addressing.</li><li>• NetBT runs NetBIOS over TCP and UDP ports 137-139 (name services, datagram transmission, session services).</li><li>• Should be disabled unless supporting legacy Windows systems or appliances.</li></ul>

# Inventory Management Servers (Slide 1 of 2)

Service	Description
<b>SNMP</b>	<ul style="list-style-type: none"><li>• Framework for managing/monitoring network devices.</li><li>• Management system and agents.</li><li>• Agent process runs on network device; maintains MIB; can initiate trap for a notable event.</li><li>• System software provides oversight location, monitors agents, displays information.</li><li>• Device queries=UDP 161; traps=UDP 162.</li></ul>
<b>Endpoint Management</b>	<ul style="list-style-type: none"><li>• Facilitates Defense in Depth security policies that require hardening to workstation level.</li><li>• Can apply OS and anti-virus updates; catalog software; apply security policies; analyze logs; monitor performance and alerts.</li><li>• Example: Microsoft's SCCM.</li></ul>
<b>syslog</b>	<ul style="list-style-type: none"><li>• Helpful to consolidate separate device logs.</li><li>• Prior to Windows 7, Windows logs were local; 3<sup>rd</sup>-party tools used to consolidate.</li><li>• Windows event subscription can forward log events to central system.</li><li>• UNIX and Linux equivalent is syslog.</li><li>• Client-server model for event collection; open format; <i>de facto</i> standard.</li></ul>

# Inventory Management Servers (Slide 2 of 2)



# Legacy and Embedded Systems

System Type	Description
<b>Embedded</b>	<ul style="list-style-type: none"><li>• Designed for a specific function.</li><li>• Range from individual microcontrollers to complex industrial control systems.</li><li>• May have been designed for a closed network, without connectivity.</li><li>• Special design and security considerations when interacting with a data network.</li><li>• Risk for maintenance and troubleshooting; require specialist knowledge.</li></ul>
<b>Legacy</b>	<ul style="list-style-type: none"><li>• No longer supported by vendor.</li><li>• May be retained on networks to support existing services that are not practical to migrate.</li><li>• Security risks.</li><li>• Should be isolated from network.</li><li>• Like embedded systems, risk for maintenance and troubleshooting; require specialist knowledge.</li></ul>



# Internet Security Appliances and Software

System Type	Description
<b>IDS/NIDS</b>	<ul style="list-style-type: none"><li>• Software and/or hardware that monitors for and quickly detects malicious behavior.</li><li>• Can also analyze and alert administrators to infrastructure problems.</li><li>• Can comprise sensors, detection software, and management software; each implementation is unique.</li></ul>
<b>IPS/NIDS</b>	<ul style="list-style-type: none"><li>• Inline security device that monitors for and blocks suspicious network and system traffic.</li><li>• May drop packets, reset connections, sound alerts; at times quarantine intruders.</li><li>• Examines packet contents.</li><li>• UTM appliance combines firewall, A-V scanner, and IDS.</li></ul>
<b>Proxy Server</b>	<ul style="list-style-type: none"><li>• Used on enterprise networks as alternative to NAT.</li><li>• Checks and forwards HTTP, email, or other requests from internal hosts to Internet; returns reply to the client.</li><li>• May be transparent (no client configuration) or non-transparent (client must be configured with proxy's IP address and port, typically 8080).</li></ul>

# Activity



Discussing Network Services  
Practice Quiz, PBQ

# Reflective Questions

1. What do you think are the most important network concepts covered in this lesson?
2. What experience do you have with any of the technologies discussed in this lesson?

