Tunneling and Gateways

Srinidhi Varadarajan

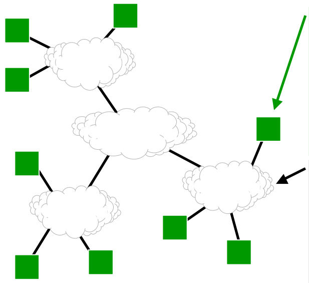
Topics

- Tunneling
  - Motivation
  - Terminology
  - Examples
- Gateways
  - Motivation
  - Interoperability
  - Remote provisioning of functionality
  - Enhanced functionality
  - Security
  - Performance improvement

Need for Tunneling and Gateways

- In a perfect networking world …
  - One set of network protocols would meet all needs
  - All systems would use this set of protocols and no others
  - When a new version is released, all systems would be instantly updated to use the new version
- But it is not a perfect world, so techniques are needed to deal with “imperfections”
  - Gateways -- usually associated with applications
  - Tunneling -- usually associated with lower levels

Networking Reality



Host Protocols
TCP/IP
DECnet
SNA
Novell
NetBEUI
…

Networks
IEEE 802.3 (Ethernet)
IEEE 802.5 (Token Ring)
IEEE 802.11
FDDI
ATM
X.25
Frame Relay
…

Interoperability (1)

- Networks are not homogeneous
  - Investment in existing equipment
  - Transitions are not instantaneous
  - Different protocols are optimal for different situations
  - Vendor support may vary or may lead to deployments that are not “technically” optimal
- Interoperability is critical in real networks
  - How does Application A use the services of Protocol X at one host and the services of Protocol Y at another host
  - How does Protocol X interact with Protocol Y within the network?

Interoperability (2)

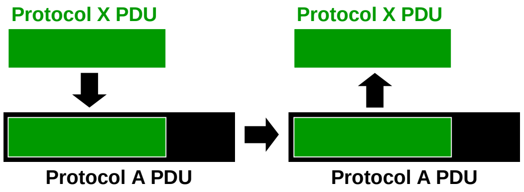
- Keys to interoperability
  - Application program interfaces that support multiple underlying services, e.g. sockets
  - Protocol design for “extensibility”
    - Generic services to simplify support for new applications
    - Separation of functionality into different protocols
    - Support for transitions to new versions, e.g. version numbers in fixed location in header

Terminology

- Gateways: Provide some form of translation between protocols at the same level
  - Translate Protocol X protocol data units (PDUs) to Protocol Y protocol data units
- Tunneling: Use a service (at the same “level”) to carry another service
  - Use Protocol Y to carry Protocol X protocol data units
- Encapsulation: Using a lower layer service
- These terms are often used interchangeably and with different meanings

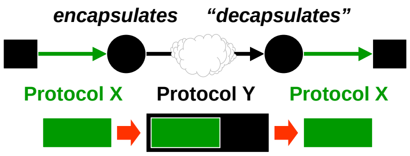
Encapsulation

- Encapsulation is simply the use of a lower level protocol data units (e.g., IEEE 802.3 frames) to carry higher layer protocol data units (e.g, IP datagrams)



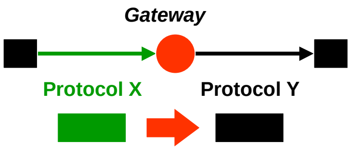
Tunneling

- Tunneling uses an alternate protocol to carry protocol data units of another protocol at the same level. Example: using IPV4 to carry IPv6 packets



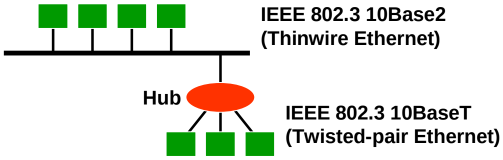
Gateways

- A gateway translates from one protocol to another, e.g. from SMTP to cc:mail.



Physical Layer Interoperability

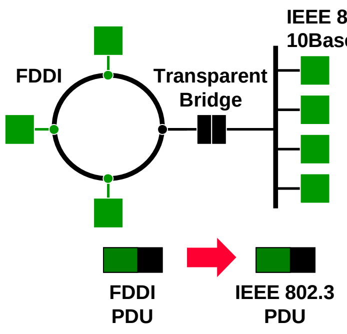
- Different physical media dependent (PMD) protocols are common
- A translation is done, but the “gateway” device is called a repeater or hub



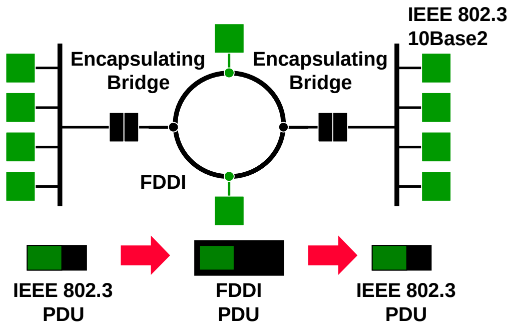
MAC Layer Interoperability (1)

- Different medium access control (MAC) protocols are also common
  - IEEE 802.2 Logical Link Control (LLC) protocol is commonly used with most MAC protocols
- Interoperability provided through
  - Translation -- supports communication between Protocol X host and Protocol Y host
  - Encapsulation -- end points must both use Protocol X, but can travel over an intermediate Protocol Y network
- Example
  - IEEE 802.3 (Ethernet)
  - Fiber Distributed Data Interface (FDDI)

MAC Layer Interoperability (2)



MAC Layer Interoperability (3)

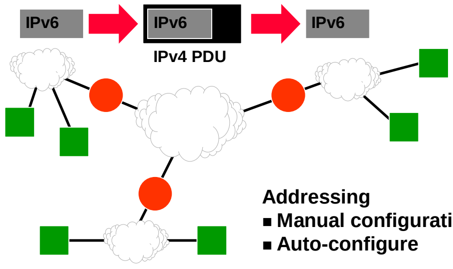


Network Layer Interoperability (1)

- Network layer interoperability is needed for
  - Transition between versions, e.g. IPv4 to IPv6
  - Enhanced functionality, e.g. multicast services provided by the Multicast Backbone (MBONE)
  - Different routing protocols
- Co-existence is related to interoperability
  - Multiple network protocols, e.g. IPX and IP, can run over the same local area network, e.g. Ethernet
  - Multi-protocol routers can route different types of network layer protocol data units

Network Layer Interoperability (2)

- 6Bone supports IPv6 connectivity across IPv4 networks



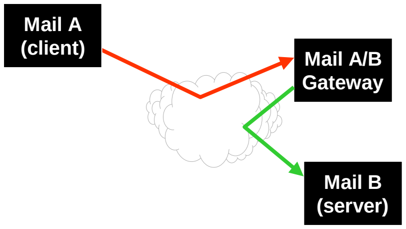
Addressing
- Manual configuration
- Auto-configure

Application Layer Interoperability (1)

- Different applications using different protocols must also interact
- Gateways -- translate between different applications providing the same service
  - Mail services using cc:Mail and SMTP (Simple Mail Transfer Protocol)
- Tunneling -- allow the use of different a underlying network
  - UDP- or TCP-based applications over an IPX network

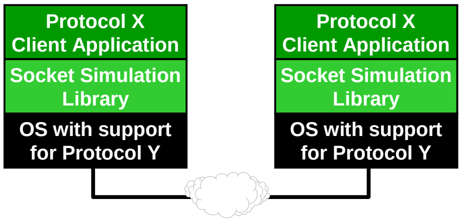
Application Layer Interoperability (2)

- Application gateway allows different applications to interoperate



Application Layer Interoperability (3)

- Application-level tunneling allows an application designed for Protocol X to operate over a network that supports only Protocol Y


Protocol X Client Application
Socket Simulation Library
OS with support for Protocol Y
Protocol X Client Application
Socket Simulation Library
OS with support for Protocol Y

Application Gateways

- An application gateway relays information between a client and a desired service
  - Gateway, in this context, is a program
  - The host running the program may be referred to as a gateway
- An edge router may also be referred to as a gateway (from a LAN to a WAN), but this is a different use of the term

Uses of an Application Gateway

- Interoperability
  - Different applications providing similar service
  - Different versions of the same service
- Support for clients with limited functionality
  - Move complexity to the gateway
- Enhanced services
  - Extending the functionality of a given protocol
- Security
  - Firewalls
- Enhance performance
  - Implement caching at the gateway

Interoperability

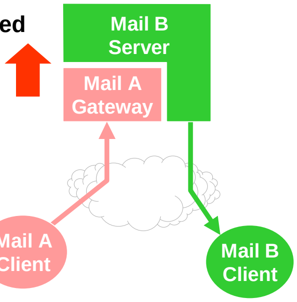
- Gateways can provide interoperability
- Example of need: electronic mail
  - Internet
    - Simple Mail Transfer Protocol (SMTP)
    - Post Office Protocol (POP)
    - Internet Message Access Protocol (IMAP)
  - Historical
    - BITNET
    - USENET
  - Proprietary
    - cc:mail
    - MCI Mail
    - others …

Mail Interoperability (1)

- Gateway allows mail to be exchanged between different types of clients and servers
- Gateway must deal with
  - Format
  - Content representation
  - Addressing

Mail Interoperability (2)

- Mail gateway often associated directly with a server

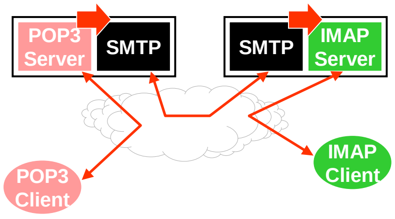


Clients With Limited Functionality

- Clients may not need full functionality
  - Complexity
  - Cost
  - Security
  - Ease-of-use (emphasis on user interface)
- Clients may not be able to provide full functionality
  - Handheld devices

SMTP with POP or IMAP

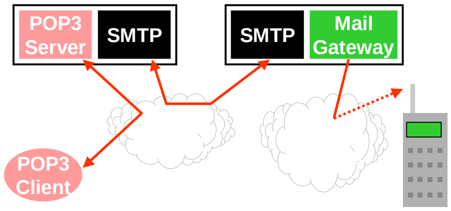
- SMTP is used to move mail through the Internet
- POP or IMAP is a simpler client-server protocol just for a mail access



POP3 Server
SMTP
SMTP
IMAP Server
POP3 Client
IMAP Client

AT&T Wireless Internet Mail Gateway

- A gateway can be used to deliver mail to very simple devices over a network other than the Internet



POP3 Server
SMTP
SMTP
Mail Gateway
POP3 Client

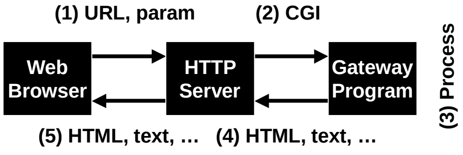
Enhanced Services

- The functionality of a protocol can be extended by a gateway
  - Client uses Protocol X to access the gateway
  - The gateway can then service client request using Protocol Y
- Common Gateway Interface (CGI) at a WWW server is an example of such an application gateway
  - Invokes a gateway program or script
  - CGI defines
    - Invocation mechanism
    - Reply mechanism

Common Gateway Interface (1)

- CGI operation
  - Client uses HTTP to transfer request to server
  - Server extracts request and invokes a gateway program (defined by CGI)
  - Gateway program processes request, possibly accessing a remote service
  - Gateway program returns result to server (defined by CGI)
  - Server returns result to clients using HTTP

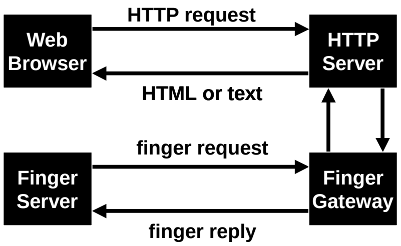
Common Gateway Interface (2)



(1) URL, param
(2) CGI
Web Browser
HTTP Server
Gateway Program
(3) Process
(5) HTML, text, …
(4) HTML, text, …

Common Gateway Interface (3)

http://xyz.vt.edu/cgi-bin/finger?xyz@cs.vt.edu

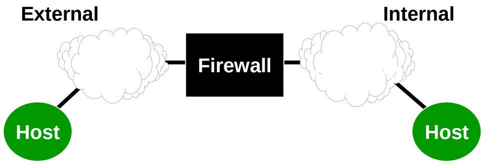


Security

- Possible security functions of a gateway
  - Separate networks for security levels
  - Control access of external hosts to internal resources
  - Control access of internal hosts to external resources
- Such a security gateway is a “firewall”
  - Firewall examines IP datagrams between a client and server to enforce a site security policy
    - Expressly permitted
    - Expressly prohibited

Firewall Topologies (1)

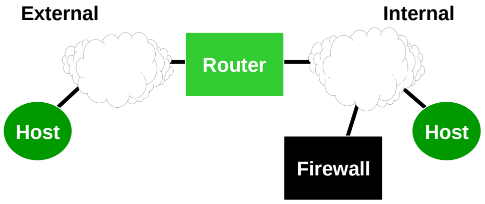
- Dual-homed firewall
  - No routed path between external and internal hosts -- bidirectional protection
  - Firewall must act as a proxy for all interactions
  - Proxy can require authentication, limit hosts, limit ports, etc.



Firewall Topologies (2)

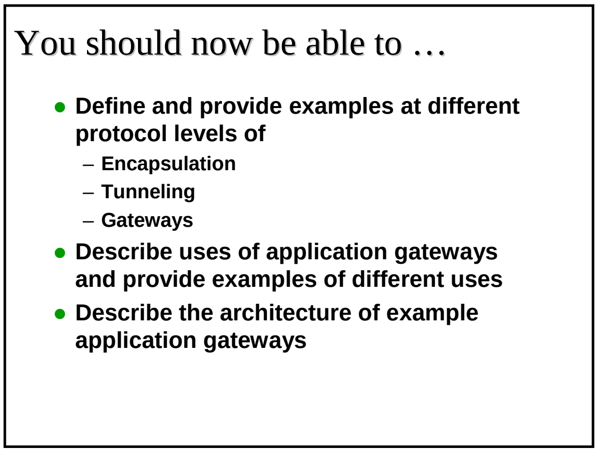
- Screened-host firewall
  - Router configured so that the firewall is the only reachable host from outside the LAN
  - Router may be varied to …
    - Allow connections *initiated* internally to go to any/limited set of external hosts
    - Limit traffic to firewall
    - Allow incoming traffic to some internal hosts, e.g. WWW server

Firewall Topologies (3)



Improving Performance

- Caching can improve the performance of the World Wide Web
  - Client-based
    - Post-fetch (in standard clients)
    - Pre-fetch (not in standard clients)
  - Server-based
    - Caching of frequently accessed files
  - Proxy-based
    - Caching of frequently accessed files
- A proxy is a form of application gateway
  - Performance by caching
  - Security as a firewall



You should now be able to …

- Define and provide examples at different protocol levels of
  - Encapsulation
  - Tunneling
  - Gateways
- Describe uses of application gateways and provide examples of different uses
- Describe the architecture of example application gateways