CS 544: Computer Networks

Dustin Ingram

June 11, 2012

1 Routing Tables & Algorithms

The three major columns of a routing table are:

1. Destination;
2. Which link to use;
3. Cost of that route.

There are three major types of routing algorithms:

1.1 Static Routing Algorithms

Static routing algorithms only have a single route to the destination. They may use shortest path routing, flooding, or flow-based routing to send data. They don't have as much need for a RT.

1.2 Dynamic Routing Algorithms

Dynamic routing algorithms attempt to be adaptive by having every network entity maintain a different routing table, and attempt to use the link with the lowest 'cost' which is determined by the algorithm. There are two major types:

- DVR – Distance Vector Routing sents the entire RT at major network events to all one's neighbors, to recompute the RT. This reacts to positive link changes quickly (new routes), but not to negative ones (links down).
- LSR – Link State Routing discovers neighbors, measures the delay to them, constructs a RT based on the information, sends this to all routers, and then computes a new RT.

1.3 Hierarchal Routing Algorithms

Hierarchical routing algorithms choose routes based on the address of the message, dividing the network into hierarchies, which only certain parts must be considered to route to them. This means that the RT size is generally smaller, but the path lengths might be much longer, as messages have to ascend and descend the entire hierarchy (e.g., mailing a letter to your neighbor must go through the central post office for distribution).

If we must expand the goal of a routing algorithm to find 2 disjoint paths to every destination, we would now have to know which portions of the network are disjoint from other parts, where there are bottlenecks (single path, therefore disjoint multi-path would be impossible), etc. Distance Vector Routing would likely be better for the task, as it would have a better overview of the entire network.

2 Routing and IPv4

IPv4 uses "hierarchical routing" to determine a route from the source to the destination. By breaking the source and destination into hierarchies, it allows the autonomous system to route to a common hierarchy first and then deal with more specific, lower level routing. There are three techniques to split the address and represent the hierarchical addressing:

1. Classful – determined by address class of IPv4 address
2. Subnetting – Like classful, but further divide the host ID
3. Subnet Mask – used to tell what portion of the address is also in the destination subnet

3 Encapsulation, Tunneling, and Translation

3.1 Encapsulation

Encapsulation is putting data from a lower-level protocol into a container for a higher level protocol. In the "railroad analogy" this is like putting a car into a railcar, so that it can be transported on the railroad and not a paved road.

3.2 Tunneling

As with the previous analogy, tunneling is the act of transporting the car, via encapsulation, across the railroad.

3.3 Translation

Translation is the changing of data encapsulation from one protocol to another. For example, it is like taking a shipping container off of a rail car and putting it onto a cargo boat. Specifically with NAT, this translates packets destined for one source to another another IP address or port.

3.4 Application

It is possible to tunnel and encapsulate a message until we push the limits of message size, etc. However, translation can only occur on the most recently encapsulated layer, as it does not concern itself with the data which the message contains.

4 Contention and Collision

Contention is two or more systems trying to use the same "media" to send data. A collision occurs when these two systems do not resolve a contention and send data simultaneously, resulting in garbage data. The two major categories of a shared MAC protocol are:

- Static, where each "station" gets a certain amount of broadcast time or bandwidth;
- Dynamic, where each "station" actively bids for the use and amount of time that they can broadcast. Subcategories of Dynamic MACs include Scheduled and Random MACs.

Within a Static MAC protocol, there is never any contention, and therefore, no collisions, as stations are specifically assigned a channel – this is the solution to this issue. In dynamic, there are two ways to deal with contention and collision: either to use some form of scheduling algorithm to determine which station can broadcast (scheduled), or randomly send when they do not notice any other station broadcasting (random).

Scheduled works well, similar to static, as some algorithm is making sure there is no contention and no collisions, however, there may be additional overhead. With a random MAC protocol, however, there may potentially be collisions due to contention, however with zero overhead.

Each take a different approach to provide support where it is needed – in most cases, this might be some type of hybrid protocol that acts like multiple types when they are needed. Contention might create issues with multiple stations, requiring algorithms to oversee assignment, however it ensures that in a shared MAC protocol each station is able to get some time to broadcast.

5 Virtual Circuits and Datagrams

5.1 Virtual Circuits

Virtual circuits are connection-oriented, where all data travels across the same path.Upon setup of the connection, a single destination address is provided. In a virtual circuit, sequencing is always in order, so higher-level applications do not have to worry about segmentation and reassembly. Routing is performed on a per-connection basis, which improves robustness and only causes bandwidth waste when the routers need to be updated about the state of the network. Flow control is possible across the network as data always takes the same path.

5.2 Datagrams

Datagrams are connectionless, where all data is independently routed within what is typically known as a packet-switched network. Because packets may take different paths through different routers, the destination address must be included in each packet, and flow control is only possible at the source and destination, resulting in some degree of wasted bandwidth in each message. Unlike in virtual circuits, sequencing is not always in order because data may arrive via different routes at different speeds.

5.3 Flow

A flow is a series of packets traveling in the same direction over a common "connection", which share information, and can identified by their:

- source IP;
- source port;
- destination IP;
- destination port;
- protocol.

or by some other form of a "flow label". A flow is similar to a route in a virtual circuit, but for a packet-switched network. A number of network protocols may result in "flows" of data. An example flow might be a stream of packets over HTTP for a streaming video service, from a server to the client. Another example is the dual-flow that is created whenever a TCP connection is created.

6 Traffic Selectors

A Traffic Selector allows a protocol to "describe" traffic, and to filter or direct it. It does this via a series of ranges and wildcards which allow for a description of various aspects of the traffic (protocol, port, IP, etc). This can be used for Quality of Service, routing, etc.
Example: IPv4 uses a form of traffic selectors to perform flow bindings

Example: QoS uses traffic selectors to support end-to-end quality of service over IP

7 Goals of Security

The seven goals of security are as follows:

1. **Authentication & Verification**
   This requires the validation and identification of a person, client, server, to prove that they are who they say they are or that information is valid.
   Example: SASL gives an authentication and security layer to other protocols, via a series of "authentication mechanisms" and challenge/response negotiation.

2. **Access Control**
   This goal involves giving the information and resources to the correct people, restricting or allowing access as necessary.
   Example: MAC provides a media access control protocol, using addressing and channels.

3. **Data Integrity**
   Used to prove that data has not been modified or changed.
   Example: SSH includes a MAC (Message Authentication Code, not to be confused with Media Access Control) in each message, which is a code produced via shared secret algorithms agreed upon by the client and server.

4. **Confidentiality**
   Protecting information so that it is available only to allowed parties.
   Example: TLS/SSL provides transport- and application-layer security via cryptography for confidentiality of network communications.

5. **Availability**
   Ensuring that a given resource will always be available to interested and allowed parties.
   Example: A reliable Persistence protocol, such as classical flooding or gossip-based algorithms.

6. **Non-Repudiation**
   Allowing a protocol transaction to only occur the intended number of times.
   Example: PGP, specifically it's certificates and certificate authorities.

7. **Trust**
   Establishing trust amongst clients/services using a protocol.
   Example: This requires a combination of previous security goals, and some notion of "trust" occurs in all aforementioned protocols.