Layer 2 Protocols

Table of Contents

Layer 2 Protocols -2 ........................................................................................................................ 2
Layer 2 Protocols -3 ........................................................................................................................ 4
Layer 2 Protocols -1 ........................................................................................................................ 6
Layer 2 Protocols -2 ........................................................................................................................ 7
Layer 2 Protocols -3 ........................................................................................................................ 8
Notices ............................................................................................................................................ 9
All right, so let’s get back to talking about Layer 2 protocols. The next ones we’ll talk about just very briefly are frame relay, and Spanning Tree Protocol. We won’t go much more into depth other than to say what they are. The frame relay protocol is a Layer 2 protocol. It helps with packet switching with Ethernet frames. There’s a low overhead, meaning there’s not much extra data sent along with it, meaning it’s a very efficient protocol and that there’s not a lot of metadata about the information that’s sent with that protocol. And it does not provide error correction. So, not a lot of
computations have to go along with receiving some frame relay packets.

Spanning tree, on the other hand, there is quite a bit of computation that happens with frame relay. And if you ever find yourself on a network and sniffing at the Layer 2 level, chances are good you'll see a lot of spanning tree protocol happen, especially if you're connected to a Cisco switch. Basically, spanning tree protocol, the software behind it, helps network devices and end hosts to detect the actual LAN topology, so to understand what the layout of a Layer 2 network looks like. And it can help calculate the best path for transmissions.

So, as you can imagine, words like calculate and detect obviously involve a lot of computation behind them to detect the best path for transmission. And what I mean when I say best path for transmission is sometimes it's the actual physically shortest path. Sometimes it's the path with the quickest response time, or the lowest latency. But spanning tree helps with that. It also helps, and this is probably the most important thing when we're talking about Layer 2, is Spanning Tree Protocol helps prevent multiple paths into loops in our Layer 2 network.
Layer 2 Protocols -3

PPTP – Point to point tunneling protocol
- PPTP → PPP → IP encapsulation for TCP/IP, IPX, and NetBEUI
- No encryption, but extended with RC4, PAP, CHAP, and EAP
- Single-factor authentication; weak implementation
- Nearly all Windows based; obsoleted by L2TP and IPSec

L2F – Layer 2 forwarding
- Tunnels at, surprise, layer 2
- Not IP dependent, supports ATM and frame relay
- Relies on PPP for authentication (designed to tunnel PPP traffic)
- Used for VPNs
- No encryption by itself

**031 Two more protocols that we’ll talk about, the point to point tunneling protocol, or PPTP. This is commonly used in conjunction with a couple Layer 3 protocols that help to set up VPNs, and help send those VPNs across LAN segments so you can VPN to places and things like this. It's mostly Windows based. There's some authentication to it, but it was proven to be weak a couple years back, point to point tunneling protocol that is, just on its own anyway. PPTP coupled with IPsec has proven to be a very effective method of doing VPNs with good authentication that's hard to crack.
And lastly, we’ll talk about L2F, or Layer 2 forwarding. Layer 2 does tunneling of Layer 2 traffic at Layer 2. Again, it’s not IP dependent. We’re just talking about Layer 2. It supports ATM networks and frame relay. And it relies on PPP, or the point to point protocol, for authentication. It is actually designed to tunnel point to point traffic. This was also used for VPNs similar to PPTP. But this doesn’t actually include any encryption on its own.

Student: So, how are these protocols, frame relay, spanning tree, PPTP, and L2F, which ones are just commonly used these days? I would think STP, but other ones, I mean, Ethernet obviously. Token ring, that’s pretty much antiquated at this point, right?

Instructor: Sure. So, and I’ll talk about my experience.

Let’s go back through these other ones.
Layer 2 Protocols -1

**Ethernet**
- Broadcast network
- Equal access
- CSMA/CD – Carrier Sense Multiple Access/ Collision Detection

**Token Ring**
- One node transmits, all receive (broadcast)
- Each node transmits in turn
- Failure in a node affects the entire ring

**029 Ethernet we use almost every day, so very commonly used.**
Layer 2 Protocols -2

Frame Relay
- Packet-switching protocol
- Lower overhead
- Does not provide error correction

Spanning Tree Protocol
- Detects LANs topology
- Calculates best path for transmission
- Prevents multiple paths and/or loops

**030 Frame relay, if you're involved with a lot of router set ups and working on the core of the Internet, I would imagine you see a lot of Layer 2 and frame relay type networks. Spanning tree protocol is used all the time. It's very, very common. I bet if we were to plug into whatever network is in this building, we'd see spanning tree protocol traffic going across because it does help speed up networks at the Layer 2 level and prevent loops.**
Layer 2 Protocols -3

PPTP – Point to point tunneling protocol
- PPTP → PPP → IP encapsulation for TCP/IP, IPX, and NetBEUI
- No encryption, but extended with RC4, PAP, CHAP, and EAP
- Single-factor authentication; weak implementation
- Nearly all Windows based; obsoleted by L2TP and IPSec

L2F – Layer 2 forwarding
- Tunnels at, surprise, layer 2
- Not IP dependent, supports ATM and frame relay
- Relies on PPP for authentication (designed to tunnel PPP traffic)
- Used for VPNs
- No encryption by itself

**031 Basically, it makes switches so we don’t have to worry about plugging the same switch into itself, and what the heck happens if we do that. It avoids all that. So, it makes devices more plug and play. Point to point tunneling protocol, I see this used quite a bit. Like I said, coupled with IPsec, which is a Layer 3 protocol for VPNs. And L2F, Layer 2 forwarding, I don’t think I’ve seen this too much at all. So, I’m just talking about my personal experiences. You asked about how common these are. I see PPTP quite a bit, but I don’t think I’ve ever seen too much of Layer 2 forwarding.
Notices

© 2015 Carnegie Mellon University

This material is distributed by the Software Engineering Institute (SEI) only to course attendees for their own individual study.

Except for the U.S. government purposes described below, this material SHALL NOT be reproduced or used in any other manner without requesting formal permission from the Software Engineering Institute at permission@sei.cmu.edu.

This material was created in the performance of Federal Government Contract Number FA8721-05-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center. The U.S. government's rights to use, modify, reproduce, release, perform, display, or disclose this material are restricted by the Rights in Technical Data-Noncommercial Items clauses (DFAR 252-227.7013 and DFAR 252-227.7013 Alternate I) contained in the above identified contract. Any reproduction of this material or portions thereof marked with this legend must also reproduce the disclaimers contained on this slide.

Although the rights granted by contract do not require course attendance to use this material for U.S. government purposes, the SEI recommends attendance to ensure proper understanding.

THE MATERIAL IS PROVIDED ON AN “AS IS” BASIS, AND CARNEGIE MELLON DISCLAIMS ANY AND ALL WARRANTIES, IMPLIED OR OTHERWISE (INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR A PARTICULAR PURPOSE, RESULTS OBTAINED FROM USE OF THE MATERIAL, MERCHANTABILITY, AND/OR NON-INFRINGEMENT).

CERT® is a registered mark owned by Carnegie Mellon University.