



Toronto Hydro Telecom

One Zone: Privacy and Security in the WiFi World

A NEW DIRECTION IN NETWORK SERVICES

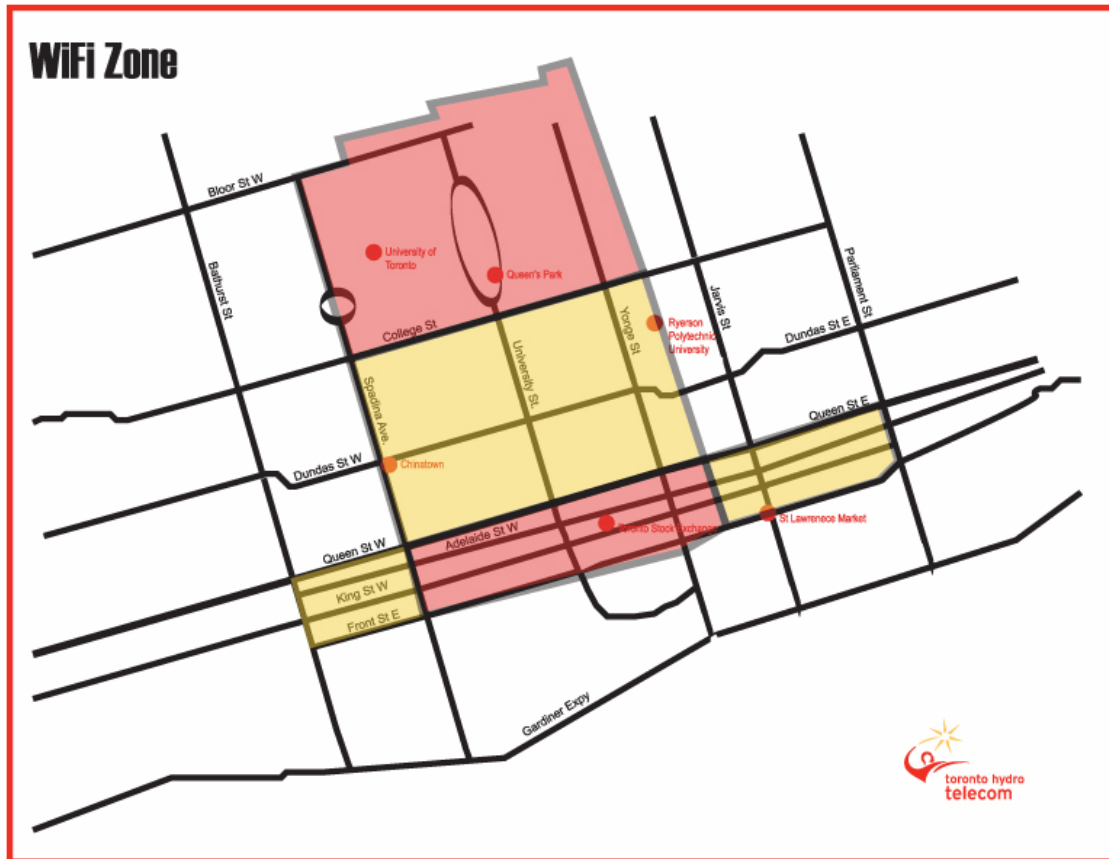


Toronto Hydro Telecom – About Us

- Competitive Telecom subsidiary of Toronto Hydro Corporation
- Data specialist – 450 km fibre optic network within Toronto, fibre connections to over 500 ‘big shiny’ buildings.
 - Customers include 4 of 6 chartered banks, insurance companies, hospitals, media companies, etc.
- Operator of Canada’s largest WiFi network – One Zone
 - Rated fastest wireless data network in North America in December 2006
- Owned by Toronto Hydro Corporation, which in turn is 100% owned by the City of Toronto

One Zone – Canada's Largest WiFi Zone

- 6 square kilometres of Wireless Internet Access – no strings attached



A NEW DIRECTION IN NETWORK SERVICES



One Zone – Nuts and Bolts

- 235 city blocks of blanketed WiFi coverage
- 225 Access Points
- 25 fibre connection points
- 200 metres radius of coverage at street level from each Access Point
- 3 types of Access Points
- Approximate weight of largest Access Point: 15 Kg
- Same frequency as baby monitors, garage door openers, cordless phones
- 70/30 split between omni-directional and directional antennae
- 6 square kilometres of blanketed coverage within 2006

WiFi Zones in the Media - Today

Potential Terror Threats to Vancouver

A Vancouver police computer crime investigator has warned that plans for a city-wide wireless Internet system puts the city at risk of terrorist attack during the 2010 Winter Olympic Games. The combination of anonymous, mobile Internet access and the potential presence of transit systems, traffic signals and gas and electric utility systems as tenants on a city-wide wireless network will make Vancouver a prime target for a paralyzing attack by hackers, said Vancouver police Det. Mark Fenton. The network would be accessible to anyone with a laptop computer and wireless Internet WiFi card. The plan calls for much of the city's infrastructure, from traffic signals and TransLink systems to BC Hydro generators and Terasen gas meters, to use the wireless platform for communications and remote operations.”

(Randy Shore, Vancouver Sun, A1)

Security Considerations/Challenges

- **Authentication** – Ensure users are properly verified on the network to deter illegal activities
 - Probably our biggest concern – privacy vs. abused children
 - EVSSL for pay system
- **Access** – Ensure that only valid uses happen
 - Harden the access network!
- **Data Privacy** – Ensure that users communications are secure
 - Only a technical challenge
 - Multiple SSID system
 - Users segregated from each other

Privacy Challenges

- How do you protect users from themselves?
 - Most don't use VPNs
 - Many have file sharing "on"
 - Many have P2P programs loaded (malware)
 - Virtually none encrypt email
- A sniffer will show the wireless packets flying....
 - A laptop with freeware (Ethereal) will completely expose your cable modem connection
- Hardening back end systems in advance of pay for service is key